全国高等职业教育计算机类规划教材·实例与实训教程系列

计算机网络技术及应用

刘枝盛　张　敏　杨　勇　主编
刘甫迎　主审

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书从介绍计算机网络基础知识入手，阐述了组成计算机网络的硬件设备、局域网技术、服务器配置、广域网技术、网络安全、网络系统集成等，使读者通过对网络技术和网络设备的了解，掌握计算机网络的架设和维护技能，并能够根据企业实际情况合理选择网络设备，组建出适合企业需求的网络。全书共 11 章，内容包括计算机网络基础知识、计算机网络硬件基础、网络操作系统、计算机局域网组网技术、Windows 网络服务器的配置与管理、广域网与网络互连技术、Internet 接入技术、计算机网络安全、网络系统集成概述、网络工程设计实例，计算机网络技术的新发展等。本书每章均配有思考题，重点内容还配有实训和实训指导。

本书可作为各高等院校相关专业的教材和各类网络技术培训学员的学习用书，还可作为网络管理者的参考用书。

图书在版编目（CIP）数据

计算机网络技术及应用 / 刘枝盛，张敏，杨勇主编．—北京：电子工业出版社，2009.6
全国高等职业教育计算机类规划教材 • 实例与实训教程系列
ISBN 978-7-121-08759-2

Ⅰ. 计…　Ⅱ. ①刘…②张…③杨…　Ⅲ. 计算机网络－高等学校：技术学校－教材　Ⅳ.TP393

中国版本图书馆 CIP 数据核字（2009）第 067962 号

策划编辑：程超群
责任编辑：张燕虹
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：16.75　字数：428 千字
印　　次：2009 年 6 月第 1 次印刷
印　　数：5 000 册　　定价：26.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

计算机网络以及 Internet 是当代发展最快的信息技术之一，是 21 世纪人才需要掌握的基本技能。

计算机网络课程的内容非常庞大和复杂，为了真正做到学以致用，提出了使学生能够“懂、建、管、用”网络的教学目标。

“懂”是理解网络原理、相关协议和标准。

“建”是掌握组建网络的工程技术。

“管”是学会管理、配置和维护网络。

“用”是在学会基本应用的基础上，学会使用将网络作为信息发布和管理的平台。

基于以上目标，我们将《计算机网络技术及应用》定位为专业基础课程，是一门理论与操作紧密结合的课程，因此，教学内容主要分为三个层面。

第一层面是计算机网络的系统知识。它涵盖了计算机网络概念，计算机网络体系结构，计算机网络的软件、硬件组成等。

第二层面是与课堂教学相对应的实训。这部分安排了一定数量的实训，对学生进行操作技能的基本训练。例如，着重介绍了交换机与路由器这两个现代网络中的重要设备，使得学生在组建网络时有必要的基础。

第三层面是结合工程项目，讲述有关计算机网络的规划、设计和应用等内容。通过实际工程项目教学，完成对基本知识和基本操作技能的综合训练，加深理解、验证、巩固课堂教学内容，使学生的知识结构更加合理，能力不断增加，综合素质不断提高。

本书的语言通俗易懂，内容丰富翔实，强调理论以够用为度，突出了以实践操作为中心的特点。

本书共 11 章，主要内容包括计算机网络基础知识、计算机网络硬件基础、网络操作系统、计算机局域网组网技术、Windows 网络服务器的配置与管理、广域网与网络互连技术、Internet 接入技术、计算机网络安全、网络系统集成概述、网络工程设计实例、计算机网络技术的新发展等。

本书由刘枝盛、张敏、杨勇担任主编，由刘甫迎担任主审，全书由刘枝盛统稿。

刘枝盛编写了第 1 章、第 2 章、第 9 章、第 10 章，张敏编写了第 4 章、第 6 章、第 7 章、第 11 章，杨勇编写了第 3 章、第 5 章、第 8 章。

本书在编写过程中参考的大量相关资料文献，均列在本书的参考文献中。对引用的这些文献资料的作者或编者深表感谢。

在本书编写过程中，国家教学名师刘甫迎教授提出了不少宝贵意见，并担任主审，在此对刘甫迎教授表示衷心的感谢。

计算机网络技术发展非常迅速，加上作者知识所限，不足之处在所难免，恳请读者批评指正。

编　者

2009 年 3 月

目　录

第 1 章　计算机网络基础知识

本章要点

计算机网络就是将分布在不同位置的具有独立操作系统的计算机以及其他附属设备用通信设备和线路连接起来，按照共同的网络协议，实现相互之间的通信和资源共享的系统。

本章讲述了计算机网络的产生与发展、计算机网络的定义和功能、计算机网络的体系结构的概念和数据通信的基本原理，为学习计算机网络做了概要性的说明。

- **本章目标**
- 了解计算机网络的产生和发展
- 理解计算机网络的定义以及计算机网络的功能
- 了解计算机网络的硬件及软件组成
- 了解计算机网络的体系结构
- 了解数据通信技术的基本技术

1.1　计算机网络的产生和发展

1.1.1　计算机网络的产生

早在计算机产生之前，人们就已经开始使用电报、电话进行通信。世界上第一台电子计算机自 1946 年问世后，在最初几年内，计算机和通信并没有什么关系，计算机一直以“计算中心”服务模式工作。1954 年，一种称为收发器（Transceiver）的终端制造出来后，人们首次使用这种终端将穿孔卡片上的数据通过电话线路传送到远方的计算机。由于当初计算机是为成批处理信息而设计的，所以当计算机在与远程终端相连时，必须在计算机上增加一个接口。显然，这个接口应当对计算机原来的硬件和软件的影响尽可能地小些。这样，就出现了所谓的“线路控制器”（Line Controller）。在通信线路的两端还必须各加上一个调制解调器。这是因为电话线路本来是为传送模拟的话音信号而设计的，它不适合于传送计算机的数字信号。调制解调器的主要作用是：把计算机或终端使用的数字信号与电话线路上传送的模拟信号进行模数或数模转换。由于在通信线路上采用的是串行传输，而在计算机内采用的是并行传输，因此线路控制器的主要功能是进行串行和并行传输的转换以及简单的差错控制。计算机主要用于成批处理数据。随着远程终端数量的增多，为了避免一台计算机使用多个线路控制器，在 20 世纪 60 年代初期，出现了多重线路控制器（Multiline Controller）。它可与许多个远程终端相连接。这种最简单的联机系统也称为面向终端的计算机通信网，是最原始的计算机网络。这里，计算机是网络的中心和控制者，终端围绕中心计算机分布在各处，而计算机的主要任务也还是进行数据的成批处理。从此，开始了计算机技术与通信技术相结合的历程。

在 20 世纪 50 年代中期，美国的半自动地面防空系统（Semi-Automatic Ground Environment，SAGE）开始了计算机技术与通信技术相结合的尝试，在 SAGE 中把远程雷达和其他测控设备的信息经由线路汇集至一台 IBM 计算机上进行集中处理与控制。世界上公认的、最成功的第一个远程计算机网络是在 1969 年，由美国国防部高级研究计划署（Advanced Research Projects Agency，ARPA）组织研制成功的。这个网络称为 ARPAnet。该网络最初主要用于军事研究目的，它主要基于这样的指导思想：网络必须经受得住故障的考验而维持正常的工作，一旦发生战争，当网络的某一部分因遭受攻击而失去工作能力时，网络的其他部分应能维持正常的通信工作。ARPAnet 在技术上的另一个重大贡献是 TCP/IP 协议组的开发和利用。ARPAnet 的试验奠定了 Internet 存在和发展的基础，较好地解决了异种机网络互连的一系列理论和技术问题。

因此，ARPAnet 成为现代计算机网络诞生的标志。

1983 年，ARPAnet 分为两部分：ARPAnet 和纯军事用的 MILnet。同时，局域网、广域网的产生和蓬勃发展对 Internet 的进一步发展起到重要的作用。其中最引人注目的是美国国家科学基金会 NSF（National Science Foundation）建立的 NSFnet。NSF 在全美国建立了按地区划分的计算机广域网并将这些地区网络和超级计算机中心互连起来。NFSnet 于 1990 年 6 月彻底取代了 ARPAnet 而成为 Internet 的主干网。

NSFnet 对 Internet 的最大贡献是使 Internet 向全社会开放，而不像以前那样仅供计算机研究人员和政府机构使用。1990 年 9 月，由 Merit、IBM 和 MCI 公司联合建立了一个非营利性组织——先进网络科学公司 ANS（Advanced Network & Science Inc.）。ANS 的目的是建立一个全美范围的 T3 级主干网，它能以 45Mbps 的速率传送数据。1991 年年底，NSFnet 的全部主干网都与 ANS 提供的 T3 级主干网相通。

Internet 的第二次飞跃归功于 Internet 的商业化，商业机构一踏入 Internet 这一陌生世界，很快发现了它在通信、资料检索、客户服务等方面的巨大潜力。于是，世界各地的无数企业纷纷涌入 Internet，带来了 Internet 发展史上的一个新的飞跃。标志着从此进入了计算机网络技术发展的新时代。

1.1.2 计算机网络的发展

计算机网络的发展大致可划分为 4 个阶段。

1．第一阶段：诞生阶段

20 世纪 60 年代中期之前的第一代计算机网络是以单个计算机为中心的远程联机系统。典型应用是由一台计算机和全美范围内 2000 多个终端组成的飞机订票系统。终端是一台计算机，其外部设备包括显示器和键盘，无 CPU 和内存。第一代计算机网络如图 1.1 所示。

随着远程终端的增多，在主机前增加了前端机（FEP）。当时，人们把计算机网络定义为“以传输信息为目的而连接起来，实现远程信息处理或进一步达到资源共享的系统”，但这样的通信系统已具备了网络的雏形。

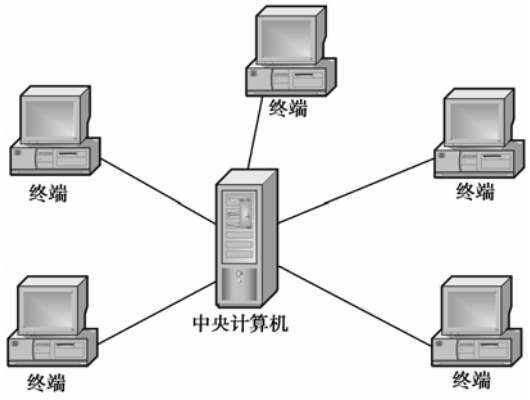


图 1.1　第一代计算机网络

2．第二阶段：形成阶段

20 世纪 60 年代中期至 70 年代的第二代计算机网络（如图 1.2 所示）是以多个主机通过通信线路互连起来，为用户提供服务的系统，兴起于 60 年代后期，典型代表是美国国防部高级研究计划署协助开发的 ARPAnet。主机之间不是直接用线路相连，而是由接口报文处理机（IMP）转接后互连的。IMP 和它们之间互连的通信线路一起负责主机间的通信任务，构成了通信子网。通信子网互连的主机负责运行程序，提供资源共享，组成了资源子网。在这个时期，网络概念为“以能够相互共享资源为目的互连起来的具有独立功能的计算机之集合体”，形成了计算机网络的基本概念。

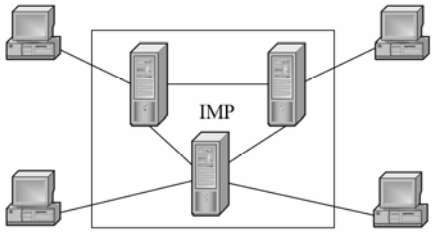


图 1.2　第二代计算机网络

3．第三阶段：互连互通阶段

20 世纪 70 年代末至 90 年代的第三代计算机网络（如图 1.3 所示）是具有统一的网络体系结构并遵循国际标准的开放式和标准化的网络。ARPAnet 兴起后，计算机网络发展迅猛，各大计算机公司相继推出自己的网络体系结构及实现这些结构的软、硬件产品。由于没有统一的标准，不同厂商的产品之间难以实现互连，人们迫切需要一种开放性的标准化实用网络环境，这样应运而生了两种国际通用的最重要的体系结构，即 TCP/IP 体系结构和国际标准化组织的 OSI 体系结构。

4．第四阶段：高速网络技术阶段

20 世纪 90 年代末至今的第四代计算机网络（如图 1.4 所示），由于局域网技术发展成熟，出现了光纤及高速网络技术、多媒体网络、智能网络，整个网络就像一个对用户透明的大型计算机系统，发展成以 Internet 为代表的互联网。

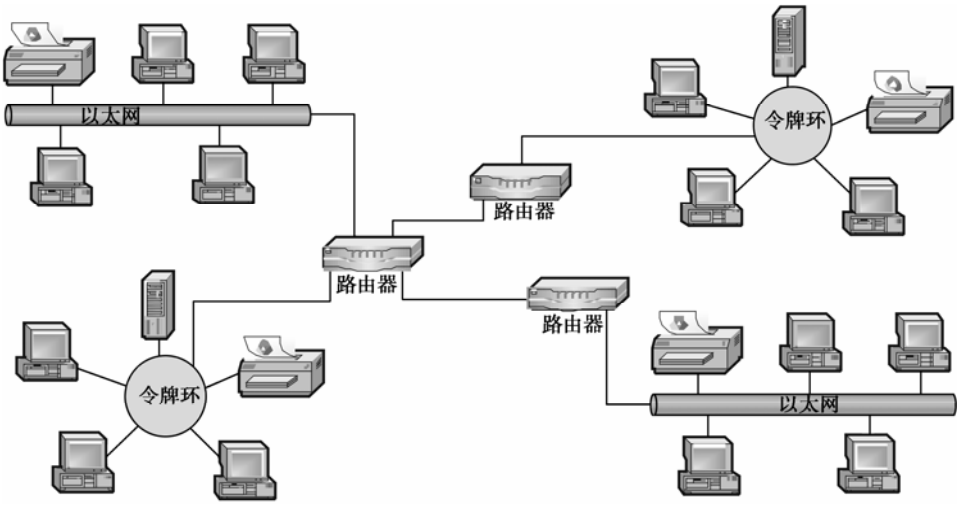


图 1.3　第三代计算机网络

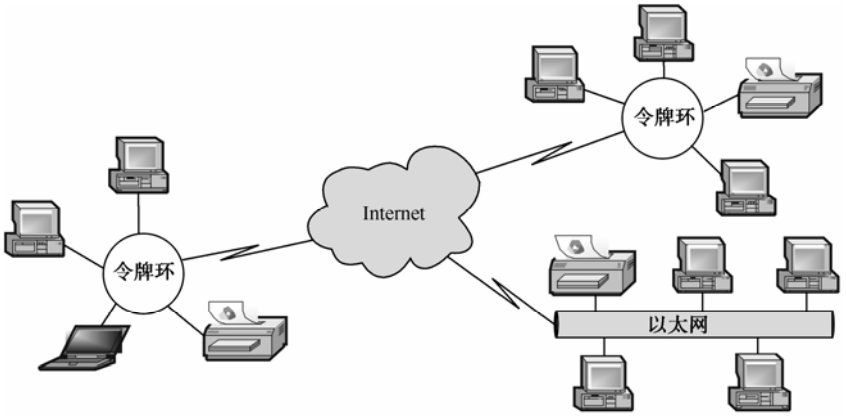


图 1.4　第四代计算机网络

从计算机网络应用来看，网络应用系统将向更深和更宽的方向发展。

（1）Internet 信息服务将会得到更大发展。网上信息浏览、信息交换、资源共享等技术将进一步提高速度、容量及信息的安全性。

（2）远程会议、远程教学、远程医疗、远程购物等应用已经逐步从实验室走出，不再只是幻想。网络多媒体技术的应用也越来越普及，成为网络发展的热点话题。

1.2　计算机网络的基本概念

1.2.1　计算机网络的定义和功能

1．计算机网络的定义

在不同时期，针对不同的应用，关于什么是计算机网络从来都有不同说法，因此，迄今为止，还没有形成计算机网络的统一定义。

简言之，计算机网络是指互连起来的能独立自主的计算机集合。

这里的“互连”意味着互相连接的两台或两台以上的计算机能够互相交换信息，达到资源共享的目的；而“独立自主”是指每台计算机的工作是独立的，任何一台计算机都不能干预其他计算机的工作。例如启动、停止等，任意两台计算机之间没有主从关系。

从这个简单定义可以看出，计算机网络涉及三个方面的问题。

（1）两台或两台以上的计算机相互连接起来才能构成网络，达到资源共享的目的。

（2）两台或两台以上的计算机连接，互相通信交换信息，需要有一条通道。这条通道的连接是物理的，由硬件实现，这就是连接介质（有时称为信息传输介质）。它们可以是双绞线、同轴电缆或光纤等“有线”介质；也可以是激光、微波或卫星等“无线”介质。

（3）计算机之间要通信交换信息，彼此就需要有某些约定和规则，这就是协议。

因此，我们可以把计算机网络定义为：把分布在不同地点且具有独立功能的多个计算机，通过通信设备和线路连接起来，在功能完善的网络软件运行下，以实现网络中资源共享为目标的系统。

2．计算机网络的功能

计算机网络具有资源共享、数据传输、集中管理、分布式处理等功能。

（1）资源共享。计算机网络最具吸引力的功能是进入计算机网络的用户可以共享网络中各种硬件和软件资源，使网络中各部分的资源互通有无、分工协作，从而提高系统资源的利用率。

（2）数据传输。数据传输是计算机网络的基本功能之一，用以实现计算机与终端或计算机与计算机之间传送各种信息，从而提高了计算机系统的整体性能，也大大方便了人们的工作和生活。

（3）集中管理。计算机网络技术的发展和应用，已使得现代办公、经营管理等发生了很大的变化。目前，已经有了许多 MIS 系统、OA 系统等，通过这些系统可以将地理位置分散的生产单位或业务部门连接起来进行集中的控制和管理，提高工作效率，增加经济效益。

（4）分布式处理。对于综合性的大型问题可以采用合适的算法，将任务分散到网络中不同的计算机上进行分布式处理，以达到均衡使用网络资源、实现分布处理的目的。

（5）负载平衡。负载平衡是指任务被均匀地分配给网络上的各台计算机。网络控制中心负责分配和检测，当某台计算机负载过重时，系统会自动将部分工作转移到负载较轻的计算机中去处理。

（6）提高安全与可靠性。建立计算机网络后，还可减少计算机系统出现故障的概率，提高系统的可靠性。另外，可将重要的资源分布在不同地方的计算机上。这样，即使某台计算机出现故障，用户在网络上仍可通过其他路径来访问这些资源，不影响用户对同类资源的访问。

1.2.2　计算机网络的分类

虽然网络类型的划分标准各种各样，但是从地理范围划分是一种大家都认可的通用网络划分标准。按这种标准可以把各种网络类型划分为局域网、城域网、广域网三种。局域网一般来说只能是一个较小区域的网，城域网是将不同地区的网络互连起来。在此要说明的是，这里的网络划分并没有严格意义上的地理范围的区分，只能是一个定性的概念。下面简要介绍这三种计算机网络。

1．局域网（Local Area Network，LAN）

局域网是最常见、应用最广的一种网络。现在，局域网随着整个计算机网络技术的发展和提高得到充分的应用和普及。几乎每个单位都有自己的局域网，有的甚至家庭中都有自己的小型局域网。局域网是在局部地区范围内的网络，它所覆盖的地区范围较小。局域网在计算机数量配置上没有太多的限制，少的可以只有两台，多的可达几百台。一般来说，在企业局域网中，工作站的数量为几十到两百台。在网络所涉及的地理距离上，一般来说可以是几米至 10km。局域网一般位于一个建筑物或一个单位内，不存在寻径问题，不包括网络层的应用。

局域网的特点是：连接范围窄、用户数少、配置容易、连接速率高。10G 以太网是目前具有最快速率的局域网。IEEE 的 802 标准委员会定义了多种主要的 LAN 网：以太网（Ethernet）、令牌环（Token Ring）网、光纤分布式接口（FDDI）网络、异步传输模式（ATM）网以及最新的无线局域网（WLAN）。

2．城域网（Metropolitan Area Network，MAN）

城域网一般来说是在一个城市，但不在同一地理小区范围内的计算机互联网。这种网络的连接距离可以为 10～100km，它采用的是 IEEE 802.6 标准。MAN 与 LAN 相比，扩展的距离更长，连接的计算机数量更多，在地理范围上可以说是 LAN 的延伸。在一个大型城市或都市地区，一个 MAN 通常连接多个 LAN，如连接政府机构的 LAN、医院的 LAN、电信的 LAN、公司企业的 LAN，等等。由于光纤连接的引入，使 MAN 中高速的 LAN 互连成为可能。

城域网多采用 ATM 技术做骨干网。ATM 是一个用于数据、语音、视频以及多媒体应用程序的高速网络传输方法。ATM 包括一个接口和一个协议，该协议能够在一个常规的传输信道上，在比特率不变及变化的通信量之间进行切换。ATM 也包括硬件、软件以及与 ATM 协议标准一致的介质。ATM 提供一个可伸缩的主干基础设施，以便能够适应不同规模、速度以及寻址技术的网络。因为 ATM 的最大缺点是成本太高，所以一般在政府城域网中应用，如用于邮政、银行、医院等。

3．广域网（Wide Area Network，WAN）

广域网也称为远程网，所覆盖的范围比城域网（MAN）更广，它一般是在不同城市之间的 LAN 或 MAN 互连，地理范围可从几百公里到几千公里。它的典型代表是 Internet。

我国 Internet 骨干网从 1996 年至今已经历了 3 个阶段：1996 年之前，多数采用 64K 至 2M 传输通道；1997—1999 年多为 2～115M 的通道；2000—2001 年从 115M 跳到 2.5G；从 2002 年开始，逐步进入 10G 时代。

2002 年 1 月 11 日，中国电信上海－杭州 10G IP over DWDM 建成开通，该通道所构建的长途波分复用传输系统，采用了思科公司长途波分复用系统和系列高速互联网路由器。这一系统已被世界各地的大型电信运营商用于构建规模庞大、运行快速稳定的“IP+Optical”网络，并被证明具有良好的稳定性、可靠性和先进性。这条全国最宽的数据通信通道的开通，标志着我国 Internet 骨干网从 2.5G 步入 10G 时代，标志着中国电信数据传输能力已经达到国际先进水平，中国电信的数据网已经成为真正的高速数据网络、海量带宽网。

目前，我国有 10 家网络运营商（即十大互联网单位），有约 200 家的跨省经营资格的网络服务提供商（ISP）。十大互联网单位分别是：

（1）中国公用计算机互联网（CHINANET）。

（2）中国科技网（CSTNET）。

（3）中国教育和科研计算机网（CERNET）。
（4）中国金桥信息网（CHINAGBN）。
（5）中国联通互联网（UNINET）。
（6）中国网通公用互联网（CNCNET）。
（7）中国移动互联网（CMNET）。
（8）中国国际经济贸易互联网（CIETNET）。
（9）中国长城互联网（CGWNET）。
（10）中国卫星集团互联网（CSNET）。

其中，非营利性单位有四家：中国科技网、中国教育和科研计算机网、中国国际经济贸易互联网和中国长城互联网。这十大互联网单位都拥有独立的国际出口。

1.2.3 计算机网络的组成

1．硬件组成

计算机网络是由两个或多个计算机通过特定通信模式连接起来的一组计算机，完整的计算机网络系统是由网络硬件系统和网络软件系统组成的。

组成一般计算机网络的硬件主要有网络服务器、网络工作站、网络适配器（又称为网络接口卡或网卡）、传输介质（主要是电缆或双绞线，还有不常用的光纤）。如果要扩展局域网的规模，就需要增加通信连接设备，如调制解调器、集线器、网桥和路由器等。把这些硬件连接起来，再安装上专门用来支持网络运行的软件，包括系统软件和应用软件，那么一个能够满足工作或生活需求的计算机网络也就建成了。图 1.5 是一个常见的企业网络结构。

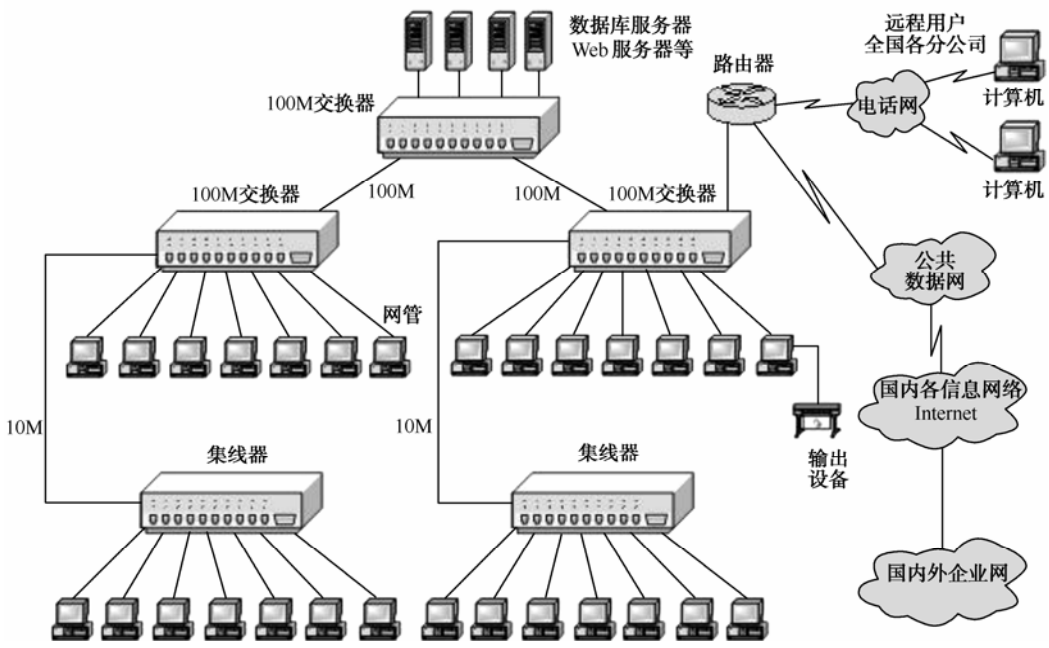


图 1.5　一个常见的企业网络结构

在计算机网络中，包含如下网络设备。

1）服务器

服务器（Server）是一台高性能计算机，用于管理网络、运行应用程序、处理各网络工作站成员的信息请示等，并连接一些外部设备如打印机、CD-ROM、调制解调器等。根据其作用的不同分为文件服务器、应用程序服务器和数据库服务器等。Internet 网管中心就有 WWW 服务器、FTP 服务器等各类服务器。

2）工作站

工作站（Workstation）也称客户机（Client），由服务器进行管理和提供服务的、连入网络的任何计算机都属于工作站，其性能一般低于服务器。个人计算机接入 Internet 后，在获取 Internet 的服务的同时，其本身就成为一台 Internet 网上的工作站。网络工作站需要运行网络操作系统的客户端软件。

3）网卡

网卡也称网络适配器、网络接口卡（Network Interface Card，NIC），在局域网中用于将用户计算机与网络相连，大多数局域网采用以太（Ethernet）网卡，如 NE2000 网卡、PCMCIA 卡等。网卡是一块插入微机 I/O 槽中，发出和接收不同的信息帧、计算帧检验序列、执行编码译码转换等以实现微机通信的集成电路卡。

4）调制解调器

调制解调器（MODEM），俗称“猫”。它是一个通过电话拨号接入 Internet 的必备的硬件设备。通常，计算机内部使用的是“数字信号”，而通过电话线路传输的信号是“模拟信号”。调制解调器的作用是，在计算机发送信息时，将计算机内部使用的数字信号转换成可以用电话线传输的模拟信号，通过电话线发送出去；在接收信息时，把电话线上传来的模拟信号转换成数字信号传送给计算机，供其接收和处理。

5）中继器和集线器

中继器（Repeater），用于连接同类型的两个局域网或延伸一个局域网。当安装一个局域网而物理距离又超过了线路的规定长度时，就可以用它进行延伸；中继器也可以收到一个网络的信号后将其放大发送到另一网络，从而起到连接两个局域网的作用。

集线器（Hub），是一种集中完成多台设备连接的专用设备，提供检错能力和网络管理等有关功能。Hub 有三种类型：对传送数据不做任何添加的 Passive Hub，称为被动集线器；能再生信号、监测数据通信的 Active Hub，称为主动集线器；能提供网络管理功能的 Intelligent Hub，称为智能集线器。

6）网桥、路由器和网关

网桥（Bridge）连接网络分支，但网桥多了一个“过滤帧”的功能。一个网络的物理连线距离虽然在规定范围内，但由于负荷很重，可以用网桥把一个网络分割成两个网络。这是因为网桥会检查帧的发送和目的地址，如果这两个地址都在网桥的这一半，那么这个帧就不会发送到网桥的另一半，这就可以降低整个网的通信负荷，这个功能称为“过滤帧”。

假如要连接两种不同类型的局域网，则需使用路由器（Router），它可以连接遵守不同网络协议的网络。路由器能识别数据的目的地地址所在的网络，并能从多条路径中选择最佳的路径发送数据。如果两个网络不仅网络协议不一样，而且硬件和数据结构都大相径庭，则需使用网关（Gateway）。

7）传输媒体

网络电缆用于网络设备之间的通信连接，常用的网络电缆有双绞线、细同轴电缆、粗同轴电缆、光缆等。此外，计算机网络还使用无线传输媒体（包括微波、红外线和激光）、卫星线路等传输媒体。

2．软件组成

1）网络操作系统

网络操作系统（NOS）是网络的心脏和灵魂，是向网络计算机提供服务的特殊的操作系统，它在计算机操作系统下工作，使计算机操作系统增加了网络操作所需要的能力。

NOS 与运行在工作站上的单用户操作系统或多用户操作系统，由于提供的服务类型不同而有差别。一般情况下，NOS 以使网络相关特性最佳为目的，如共享数据文件、软件应用以及共享硬盘、打印机、调制解调器、扫描仪和传真机等。

为防止一次由一个以上的用户对文件进行访问，一般网络操作系统都具有文件加锁功能。文件加锁功能可跟踪使用中的每个文件，并确保一次只能由一个用户对其进行编辑。文件也可由用户的口令加锁，以维持专用文件的专用性。

NOS 还负责管理 LAN 用户和 LAN 打印机之间的连接。NOS 总是跟踪每一个可供使用的打印机以及每个用户的打印请求，并对如何满足这些请求进行管理，使每个终端用户的操作系统感到所希望的打印机犹如与其计算机直接相连。

NOS 还对每个网络设备之间的通信进行管理，这是通过 NOS 中的媒体访问法来实现的。

NOS 的各种安全特性可用来管理每个用户的访问权力，确保关键数据的安全保密。因此，NOS 从根本上说是一种管理器，用来管理连接、资源和通信量的流向。

现在常用的 NOS 有 Novell NetWare、Windows NT、UNIX 和 Linux 等。

2）网络协议和应用服务软件

协议是网络设备之间进行互相通信的语言和规范。常用的网络协议有：IPX、TCP/IP、NetBEUI、NWLink。TCP/IP 是 Internet 使用的协议。

客户机（网络工作站）上使用的应用软件通称为客户软件。它用于应用和获取网络上的共享资源。用在服务器上的服务软件则使网络用户可以获取这种服务。

客户机/服务器系统的引入，给许多桌面系统注入了新的活力。例如电子消息系统（又称群件系统，Groupware），利用计算机和通信网络在工作组内协调和管理工作进程。目前的 Lotus Notes、Microsoft Exchange Server 等都使用了客户机/服务器概念，在降低客户机内存负担的同时，提高了效率。

3．通信子网和资源子网

在逻辑上，又可以将计算机网络看成是由通信子网和资源子网两个子网组成的。

计算机网络首先是一个通信网络，各计算机之间通过通信媒体、通信设备进行数字通信。在此基础上，各计算机可以通过网络软件共享其他计算机上的硬件资源、软件资源和数据资源。从计算机网络各组成部件的功能来看，各部件主要完成两种功能，即网络通信和资源共享。把计算机网络中实现网络通信功能的设备及其软件的集合称为网络的通信子网，而把网络中实现资源共享功能的设备及其软件的集合称为资源子网。计算机网络逻辑组成示意图如图 1.6 所示。

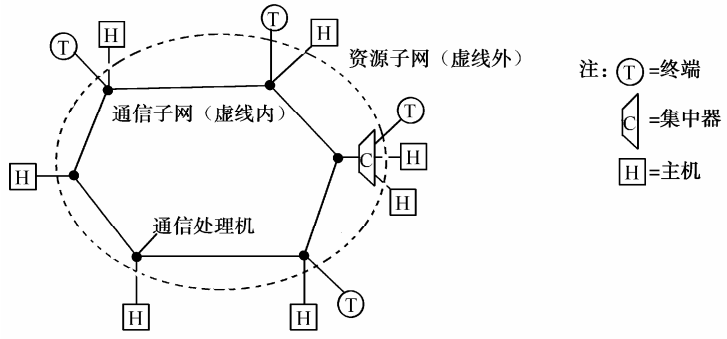


图 1.6　计算机网络逻辑组成示意图

1.2.4　计算机网络的应用

计算机网络在资源共享、数据传输、分布式处理、高可靠性、高性价比和易扩充性等方面所具有的特殊优势，使得它在工业、农业、交通运输、邮电通信、文化教育、商业、国防以及科学研究等各个领域、各个行业获得了越来越广泛的应用。下面简要介绍计算机网络在一些具有普遍意义和典型意义领域中的应用。

1．文件共享与网络打印

打印服务能对网络打印进行管理与控制，允许多人同时访问打印设备。为实现这些功能，网络操作系统使用了“打印队列”的概念，这是一种特殊的存储区域。该区域保存了打印作业，所有作业按一定的顺序传送到打印机。计算机将打印信息输出至打印队列的时候，实际上类似于将信息送到打印机。打印作业简单地存储到打印队列中，排在前面的打印作业由打印机输出后，自己再实际地转发给打印机。

利用文件服务器提供的服务，网络用户可以共享文件。文件服务其实是一些网络应用程序，它们能保存、取回和移动数据。这种类型的服务或许正是各大公司纷纷投资于网络建设的一项重要原因。利用网络文件服务，用户可以交换、读取、写入和管理共享文件以及其中包含的数据。经特殊设计后，文件服务器可出色地支援网络文件服务。

2．管理信息系统（MIS）应用

企业管理信息综合环境是一种全新概念的开放的现代管理和办公环境，它以 TCP/IP 广域网互连、路由、防火墙和网络管理技术为核心，建立一个安全可靠的广域网络应用平台；利用世界最新的 Intranet、HTML 超文本链信息融合、图文并茂的多媒体开放文档体系结构、交互式对象（Interactive Object）、虚拟机以及中西文全文检索技术为基础，建立一个开放的信息资源管理平台；利用安全可靠的数字签名身份验证和加密技术、先进的消息传递和工作流管理平台；利用 Client/Sever、数据库及分布式处理技术构架事务处理平台。

3．办公自动化系统（OA）

办公自动化系统（OA）是针对办公室环境，借助计算机和计算机网络技术用以改善办公室条件、辅助办公人员提高业务的工作效率和质量。

OA 应用能够对工作流程提供良好的支持，并根据不同的情况，不同的工作状态采取不同的措施，能更好地跟踪工作执行情况，满足下情上传、上令下达的时效性。OA 应用可建立高效的现代化企业办公环境，实现公文收发流转、签发、归档等群组作业效果；可连接企业各个岗位人员，连接企业各类信息资源（包括打字、录入、排版、编辑）等个人事务处理。

开发工作流应用，需集成数据库及 Web 应用，乃至 Office 办公软件，提供先进的信息加工处理手段，并为起草公文人员提供充足良好的基础数据源和编辑环境，完成工作流程处理过程，开始步入无纸办公时代。

4．电子商务应用

电子商务系统，主要包括电子信息公布、网上谈判、商品交易几部分。电子信息公布可以采用信息检索的方式，电子商务系统提供最方便的信息检索手段。网上谈判一般采用 EDI 方式，也可采用 Web Phone 的方式。在完善的系统中，应该有这两种方式，特别是对于合同单的传送，EDI 是必需的。一旦合同单已经签订，就进入商品交易阶段，交易双方将交易信息传到银行，银行对双方认证后进行账户间的资金转移。为了安全，EDI 进行数据传输时采用密文传输。电子商务系统是一个综合系统，它集合了计算机技术、网络通信技术、金融信息处理技术等。

5．远程教育

远程教育即 Internet 网上教育，它是指跨越地理空间进行教育活动。远程教育涉及各种教育活动，包括授课、讨论和实习。Internet 的普及和广泛使用极大地增加了进行远程教育的可能。

远程教育的出现，克服了传统教育在空间、时间、受教育者年龄和教育环境等方面的限制，满足了社会对学习文化的需求，使得计算机时代的教育变得更加人性化和多样化。

远程教育的出现，使教育的目标不再是一张文凭，而是为了终身受教育。互联网的普及带来了崭新的学习模式，随着信息化、网络化水平的提高，它将使传统的教育发生巨大的变化。

1.3 计算机网络体系结构

1.3.1 网络体系结构的概念

计算机网络体系结构是指整个网络系统的逻辑组成和功能分配，它定义和描述了一组用于计算机及其通信设施之间互连的标准和规范的集合，换言之，计算机网络体系结构就是使这个计算机网络及其部件所应该完成的功能的精确定义。这些功能究竟由何种硬件或软件完成，则是一个遵循这种体系结构的实现的问题。可见，体系结构是抽象的，而实现是具体的，是运行在计算机软件和硬件之上的。

世界上第一个网络体系结构是美国 IBM 公司于 1974 年提出的，它取名为 SNA（System Network Architecture，系统网络体系统结构）。凡是遵循 SNA 的设备就称为 SNA 设备。这些 SNA 设备可以很方便地进行互连。在此之后，很多公司也纷纷建立自己的网络体系结构，这些体系结构大同小异，都采用了层次技术，但各有其特点以适合本公司生产的计算机组成网络，这些体系结构也有其特殊的名称，如 20 世纪 70 年代末有美国数字网络设备公司（DEC 公司）发布的 DNA（Digital Network Architecture，数字网络体系结构）等。但是，使用不同体系统结构的厂家设备是不可以相互连接的。后来，经过不断地发展，诞生了以下的体系结构，从而实现了不同厂家设备的互连。

计算机网络体系结构包括 3 部分内容，即参考模型、协议规范、服务定义，其中最重要的是协议规范。狭义地讲，计算机网络体系结构就是协议规范（简称协议）。因此，不仅要学

习研究计算机网络中的硬件和软件，更要学习研究协议。

最重要的计算机网络体系结构标准是 OSI 与 TCP/IP。

1.3.2 ISO/OSI体系结构标准

为了实现不同厂家生产的计算机系统之间以及不同网络之间的数据通信，国际标准化组织（ISO）对各类计算机网络体系结构进行了研究，它定义了网络互连的 7 层框架，这就是开放系统互连参考模型（OSI/RM），也称为 ISO/OSI。

这里的“开放”是指只要遵循 OSI 标准，一个系统就可以与位于世界上任何地方、同样遵循 OSI 标准的其他任何系统进行通信。

OSI 参考模型的最高层为应用层，面向用户提供网络应用服务；最底层为物理层，与通信介质相连实现真正的数据通信，如图 1.7 所示。除物理层之外，其余各对等层之间均不存在直接的通信关系，而是通过各对等层的协议来进行通信。只有两个物理层之间通过通信介质进行真正的数据通信。

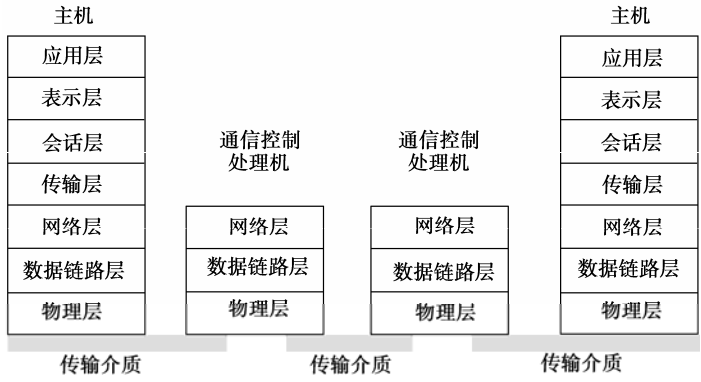


图 1.7　ISO/OSI 体系结构标准示意图

1．物理层（Physical Layer）

物理层的主要任务是透明地传送二进制比特流，但是物理层并不关心比特流的实际意义和结构，只是负责接收和传送比特流。物理层的另一个任务是定义网络硬件的特性，包括使用什么样的传输介质，以及与传输介质连接的接头等物理特性。

2．数据链路层（Data Link Layer）

数据链路层传输数据的单位是帧，其主要任务是通过数据链路层协议，在不太可靠的物理链路上实现可靠的数据传输。由于物理层仅仅接收和传送比特流，并不关心比特流的意义和结构，所以数据链路层要产生和识别数据帧的边界。另外，数据链路层还提供了差错控制与流量控制的方法，以保证在物理线路上传送的数据无差错。

3．网络层（Network Layer）

网络层传送的数据单位是报文分组或包。网络层的关键问题是如何进行路由选择，使发送站的传输层所传下来的报文能够正确无误地交付给目的站的传输层。路由选择的好坏在很大程度上决定了网络的性能，如网络吞吐量、平均延迟时间、资源的有效利用率等。

另外，如果在子网中同时出现的数据分组太多，它们将互相阻塞，影响数据的正常传输。因此，拥塞控制也是网络层的功能之一。

4．传输层（Transport Layer）

传输层所传送的数据单位是报文。传输层是通信子网（下面 3 层）和资源子网（上面 3 层）的分界线，它屏蔽了传输层以下的数据通信细节，使高层用户感觉不到通信子网的存在。传输层的主要功能是从会话层接收数据报文，并且在发送的报文较长时，在传输层先把它分割成若干个报文分组，然后再交给它的下一层（即网络层）进行传输。另外，这一层还负责报文错误的确认和恢复，以确保信息的可靠传递。

5．会话层（Session Layer）

会话层允许不同机器上的用户建立会话关系，它主要针对远程访问，其目的是完成正常的数据交换，并提供了对某些应用的增强服务会话。会话层的主要任务包括会话管理、传输同步以及数据交换管理等。会话一般都是面向连接的，例如，当文件传输到中途时建立的连接突然断了，是从文件的开始重传还是断点续传，这个任务由会话层来完成。

6．表示层（Presentation Layer）

表示层关心的是所传输的信息的语法和语义，但它仅完成语法的处理，而语义的处理是由应用层来完成的。表示层的主要功能有：用于处理在多个通信系统之间交换信息的表示方式，包括数据格式的变换、数据加密与解密、数据压缩与恢复等。

7．应用层（Application Layer）

应用层是 OSI 网络体系结构的最高层，是计算机网络与最终用户的界面，为网络用户之间的通信提供专用的程序。OSI 的 7 层协议从功能划分来看，下面 6 层主要解决支持网络服务功能所需要的通信和表示的问题，而应用层则提供完成特定网络功能服务所需要的各种应用协议，如文件传输（FTP）、电子邮件（E-mail）、网络管理、远程登录等。

1.3.3　TCP/IP体系结构标准

TCP/IP 体系结构的实现称为 TCP/IP 协议栈。OSI 参考模型研究的初衷是，希望为网络体系结构与协议的发展提供一种国际标准，但由于 Internet 在全世界的飞速发展，使得 TCP/IP 得到了广泛的应用，虽然 TCP/IP 不是 ISO 标准，但广泛的使用也使 TCP/IP 成为一种“实际上的标准”，并形成了 TCP/IP 参考模型。TCP/IP 在不断发展的过程中也吸收了 OSI 标准中的许多概念及特征。

TCP/IP 是四层的体系结构：应用层、传输层、网际层和网络接口层，如图 1.8 所示。

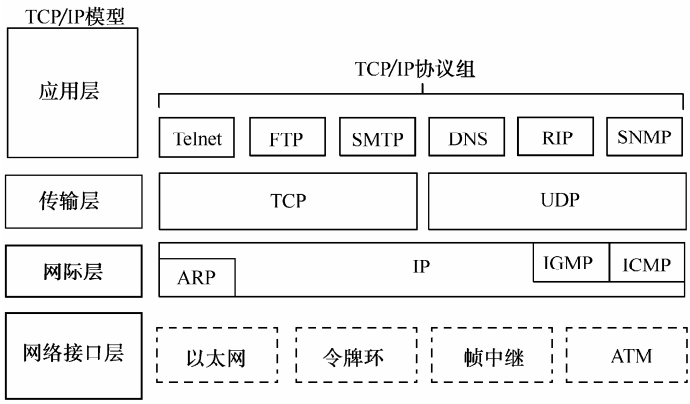


图 1.8　TCP/IP 体系结构标准

1．网络接口层（或称主机—网络层）

网络接口层与 OSI 参考模型的物理层和数据链路层相对应，它不是 TCP/IP 的一部分，但它是 TCP/IP 赖以存在的与各种通信网之间的接口。TCP/IP 对网络接口层并没有给出具体的规定。在主机—网络层中包含了多种网络层协议，如以太网（Ethernet）协议、令牌环（Token Ring）网协议等。

2．网际层

网际层是整个 TCP/IP 参考模型的关键部分，它提供的是无连接的服务，主要负责将源主机的数据分组（Packet）发送到目的主机。网际层上有四个主要的协议：网际协议（IP）、Internet 控制报文协议（ICMP）、地址解析协议（ARP）等。

3．传输层

与 OSI 的传输层类似，TCP/IP 参考模型中的传输层主要负责主机到主机之间的端对端通信。该层定义了两个端到端的协议，即 TCP（传输控制协议）和 UDP（用户数据协议）。其中，TCP 是面向连接的服务，UDP 是无连接的服务。

面向连接的服务，就是在数据交换之前，必须先建立连接；在数据交换结束后，应终止这个连接。面向连接的服务具有建立连接、数据传输和释放连接三个阶段，数据在传送时是按序传送的。在无连接服务的情况下，两个实体之间的通信不需要先建立好一个连接，因此其下层的有关资源不需要事先进行预定保留，而是在数据传输时动态地进行分配。

4．应用层

在 TCP/IP 体系结构中并没有 OSI 的会话层和表示层，TCP/IP 把它都归结到应用层。应用层负责向用户提供一组常用的应用程序，如电子邮件、远程登录、文件传输等。应用层包含了所有 TCP/IP 协议组中的高层协议，如文件传输协议（FTP）、简单电子邮件传输协议（SMTP）、域名系统（DNS）等。

TCP/IP 是事实上的工业标准。它具有很强的灵活性，支持任意规模的网络，几乎可连接所有类型的服务器和工作站，同时，它还是多种通信设备的配置工具。

1.3.4 局域网体系结构标准

1．IEEE 802 标准

为了使不同厂家生产的局域网能够相互连通进行通信，IEEE 于 1980 年 2 月下设了一个 802 委员会，专门从事局域网、城域网标准的制订，形成的一系列标准统称为 IEEE 802 标准。ISO 于 1984 年 3 月将它作为局域网、城域网的国际标准系列，称为 ISO 8802 标准。

IEEE 802 标准主要涉及物理层、数据链路层以及网络层的一部分。在 IEEE 802 标准中，将 OSI/RM 的数据链路层分为 MAC 及 LLC 两个子层。

MAC（Media Access Control，介质访问控制子层），负责解决设备使用共享信道的问题。LLC（Logical Link Control，逻辑链路控制子层），负责完成通常意义下的数据链路层功能，如差错控制、流量控制等。

2．IEEE 802 标准的功能与相关标准

局域网可采用多种传输介质与拓扑，相应的介质访问控制方法就有多种。将数据链路层分成两个子层，只要设计合理，使 MAC 子层向上提供统一的服务接口，就能将底层的实现细节完全屏蔽掉，即不同的物理网络，物理层与 MAC 子层不同，而 LLC 子层相同，网络的上层协议可运行于任何一种 IEEE 802 标准的局域网上。这种分层方法也使 IEEE 802 标准具

有良好的可扩充性，可以很方便地接纳新的介质与介质访问控制方法。

3．IEEE 802 标准系列

802.1：体系结构和桥接。

802.2：逻辑链路控制（LLC）。

802.3：CSMA/CD 总线网的 MAC 和 PHY 规范。

802.4：令牌总线网的 MAC 和 PHY 规范。

802.5：令牌环网的 MAC 和 PHY 规范。

802.6：城域网 DQDB 的接入方法和物理层规范。

802.7：宽带技术。

802.8：光纤技术。

802.9：综合话音数据局域网（Voice/Data Integration）。

802.11：无线局域网（WLAN）的 MAC 和 PHY 规范。

802.12：优先级高速局域网（100BaseVG AnyLan）。

802.14：电缆电视（Cable-TV）网上的数据传输。

802.15：无线个人网（WPAN/Bluetooth）。

802.16：宽带无线接入（BWA, i.e. Wireless MAN）。

802.17：弹性分组环（Resilient Packet Ring）。

802.18：无线电调整（Radio Regulatory）。

802.19：共存（Coexistence）。

802.10：可互操作的 LAN/MAN 安全。

802.20：移动宽带无线访问（MBWA，i.e. Wireless Mobility）。

1.4 数据通信技术简介

1.4.1 基本概念

数据通信的目的就是传递信息。一次通信中产生和发送信息的一端称为信源，接收信息的一端称为信宿。通信线路称为信道，信源和信宿之间的信息交换是通过信道进行的。

信息可以用模拟信号或数字信号来进行传输，它的一般形式可以用图 1.9 来概括。

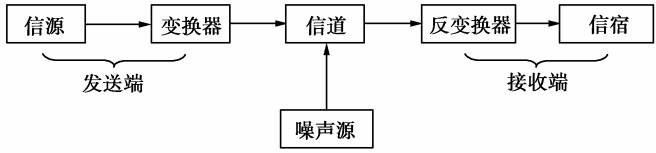


图 1.9 通信系统的模型

发送端信源的作用是把各种可能信息转换成原始电信号，为了使这个原始电信号适合在信道上传输，就要通过变换器转换成适合在信道上传输的信号。信道是信号的传输媒介及有关的设备（如中继器等）。通过信道传输到远地的电信号先由接收端的反变换器转换复原成原始的信号，再送给接收者（信宿），而后由信宿将其转换成各种信息。在图 1.9 中，噪声源是信道中噪声（即对信号的干扰）以及分散在通信系统其他各处的噪声的集中表示。

信号（Signal）是携带信息的载体。信号在通信系统中可分为模拟信号和数字信号。模拟信号是指一种连续变化的电信号。数字信号是指一种离散变化的电信号。

如果信源产生的是模拟数据且以模拟信道传输，则叫做模拟通信；如果信源发出的是模拟数据而以数字信号的形式进行传输，那么这种通信方式叫做数字通信。

如果信源发出的是数字数据，则可有两种传输方式。这时，无论是用模拟信号传输或是用数字信号传输都叫做数据通信。

1.4.2 数据通信

数据通信是通信技术和计算机技术相结合而产生的一种新的通信方式。

数据是预先约定的具有某种含义的任何一个数字或一个字母（符号）以及它们的组合。

数据通信的任务是以可靠高效的手段来传输信号，涉及的内容包括信号传输、传输媒体、信号编码、接口、数据链路控制以及信道复用。数据通信技术是计算机网络通信技术的支撑技术，它依照通信协议，利用数据传输技术在两个功能单元之间传递数据信息，它可实现计算机与计算机、计算机与终端、终端与终端之间的数据信息传递。

要在两地之间传输信息，必须有传输信道，根据传输媒体的不同，有有线数据通信与无线数据通信之分。但是，它们都是通过传输信道将数据终端与计算机连接起来，而使不同地点的数据终端实现软、硬件和信息资源的共享。

1．有线数据通信

有线数据通信技术网络很多，以下列举的是其中的三种。

1）数字数据网（DDN）

数字数据网由用户环路、DDN 节点、数字信道和网络控制管理中心组成。DDN 是利用光纤或数字微波、卫星等数字信道和数字交叉复用设备组成的数字数据传输网。也可以说，DDN 是把数据通信技术、数字通信技术、光纤通信技术以及数字交叉连接技术结合在一起的数字通信网络。数字信道应包括用户到网络的连接线路，即用户环路的传输也应该是数字的，但实际上也有普通电缆和双绞线，其传输质量差些。

2）分组交换网

因为分组交换公用数据网（PSPDN）是以 CCITT X．25 建议为基础的，所以又称为 X.25 网。它采用存储—转发方式，将用户送来的报文分成具有一定长度的数据段，并在每个数据段上加上控制信息，构成一个带有地址的分组组合群体，在网上传输。分组交换网最突出的优点是，在一条电路上同时可开放多条虚通路，供多个用户同时使用，网络具有动态路由选择功能和先进的误码检错功能，但网络性能较差。

3）帧中继网

帧中继网络通常由帧中继存取设备、帧中继交换设备和公共帧中继服务网 3 部分组成。帧中继网是由分组交换技术发展起来的。帧中继技术把不同长度的用户数据组均包封在较大的帧中继帧内，加上寻址和控制信息后在网上传输。

2．无线数据通信

无线数据通信也称移动数据通信，它是在有线数据通信的基础上发展起来的。有线数据通信依赖于有线传输，因此只适合于固定终端与计算机或计算机之间的通信。移动数据通信是通过无线电波的传播来传送数据的，因而有可能实现移动状态下的移动通信。狭义地说，移动数据通信就是计算机之间或计算机与人之间的无线通信。它通过与有线数据网互连，把

有线数据网路的应用扩展到移动和便携用户。

1.4.3 数据通信方式

1．单工通信、半双工通信和全双工通信

按照数据在信道上的传输方向，可分为单工通信、半双工通信和全双工通信三种，如图 1.10 所示。

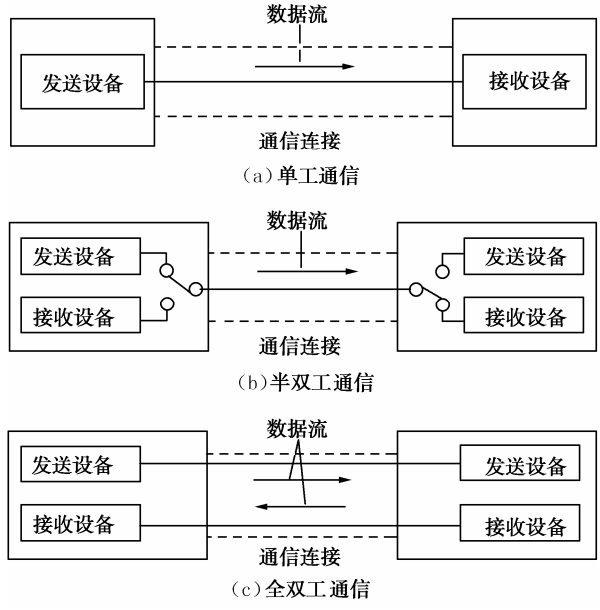


图 1.10　数据通信方式

单工数据传输只支持数据在一个方向上传输。

半双工数据传输允许数据在两个方向上传输，但是，在某一时刻，只允许数据在一个方向上传输，它实际上是一种切换方向的单工通信。

全双工数据通信允许数据同时在两个方向上传输，因此，全双工通信是两个单工通信方式的结合，它要求发送设备和接收设备都有独立的接收和发送能力。

2．并行通信传输及串行通信传输

按同一时刻传送的数据位，又可以把数据通信方式分为并行通信传输及串行通信传输方式，如图 1.11、图 1.12 所示。

并行通信传输中有多个数据位，同时在两个设备之间传输。发送设备将这些数据位通过对应的数据线传送给接收设备，还可附加一位数据校验位。接收设备可同时接收到这些数据，不需要做任何变换就可直接使用。并行方式主要用于近距离通信。计算机内的总线结构就是并行通信的例子。这种方法的优点是传输速度快、处理简单。

串行通信传输时，数据是一位一位地在通信线上传输的，先由具有几位总线的计算机内的发送设备，将几位并行数据经并—串转换硬件转换成串行方式，再逐位经传输线到达接收设备中，并在接收端将数据由串行方式重新转换成并行方式，以供接收方使用。串行通信传输的速度比并行传输慢得多，但对于覆盖面极其广阔的公用电话系统来说具有更大的现实意义。

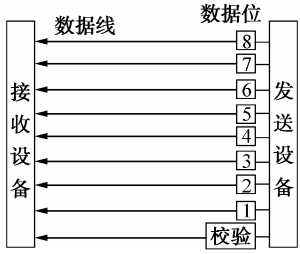


图 1.11　并行通信传输

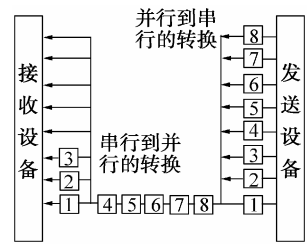


图 1.12　串行通信传输

并行传输的特点是传输速度快，在一个比特时间内可传输一个字符，但通信成本高，每个比特传输要求一个单独的信道支持。

串行传输特点是传输速度低，一次一个比特，但通信成本较低，只需一个信道。

3．异步传输和同步传输

所谓同步的意思是指信息收、发双方在时间上的协调一致性。按同步技术的不同，数据传输可以分为异步传输和同步传输。

在异步传输方式中，一次只传输一个字符。每个字符用一位起始位引导、一位停止位结束。在没有数据发送时，发送方可发送连续的停止位。接收方根据“1”至“0”的跳变来判断一个新字符的开始，然后接收字符中的所有位。

同步传输时，为使接、收双方能判别数据块的开始和结束，还需要在每个数据块的开始处和结束处各加一个帧头和一个帧尾，加有帧头、帧尾的数据称为一帧。

4．数据通信的主要技术指标

1）信息传输速率（R_b）

信息传输速率又称信息速率、比特率，它表示单位时间（每秒）内传输实际信息的比特数，单位为比特 / 秒，记为 b/s 或 bps。

2）码元传输速率（R_B）

码元传输速率又称波特率或调制速率。它表示单位时间（每秒）内信道上实际传输码元的个数，单位是波特（Baud），用符号“B”来表示。

信息传输速率 R_b 与码元传输速率 R_B 之间的关系为：

$$R_b = R_B \log_2 N$$

式中，N 为码元的进制数。

【例 1.1】　采用四相调制方式，即 $N=4$，并且信号周期 $T=833\times10^{-6}$s，求它的信息传输速率（R_b）及码元传输速率（R_B）。

【解】码元传输速率 R_B 即信号频率，它与信号周期互为倒数，所以：

$R_B = 1/T = 1/(833\times10-6) = 1200$（Baud）

则：

$R_b = 1/T \cdot \log_2 N = 1/(833\times10-6)\times\log24 = 2400$（bps）

3）误码率

误码率是指二进制码元在数据正常传输过程中出错的概率，也称为“出错率”，常用 P_e 表示。P_e 的定义公式如下：

$$P_e = n_e/n$$

n 为传输的二进制代码总数，n_e 表示接收中传错的码元数。

4）时延（Delay）

时延又称为延迟，是指一个分组从发送端开始发送到接收端接收所需的时间。数据传输总时延等于发送时延、传播时延和处理时延的总和。

1.4.4 数据通信的交换方式

计算机网络的通信子网部分是利用中间节点将通信双方连接起来的。

中间节点指用于数据交换的中间设备，中间节点又称交换设备。它不关心被传输的数据内容，仅执行交换的动作，起数据交换的功能，将数据从一个端口交换到另一端口，继而传输到另一台中间节点，直至目的地。站点是指发送和接收数据的终端设备。

1．数据通信的交换方式

数据通信的交换方式如图 1.13 所示。

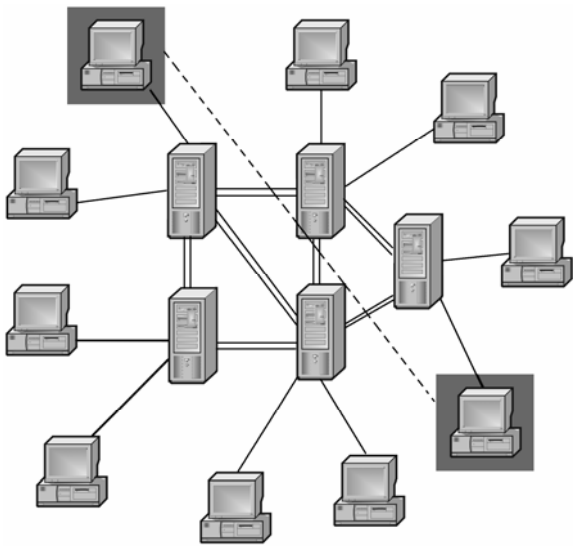


图 1.13　数据通信的交换方式

信息通过中间节点交换可以采用不同的技术。通常使用的有以下三种通信交换技术。

（1）电路交换。电路交换是指两台计算机或终端在相互通信时，使用同一条实际的物理链路，通信中自始至终使用该链路进行信息传输，并且不允许其他计算机或终端同时共享该链路。

（2）报文交换。报文交换是将用户的报文存储在交换机的存储器（内存或外存）中，当所需输出电路空闲时，再将该报文发往需接收的交换机或终端。这种存储—转发的方式可以提高中继线和电路的利用率。

（3）分组交换。分组交换是将用户发来的整份报文分割成若干个定长的数据块（称为分组或打包），将这些分组以存储—转发的方式在网内传输。第一个分组信息都连有接收地址和发送地址的标志。在分组交换网中，因为不同用户的分组数据均采用动态复用的技术传送，即网络具有路由选择，同一条路由可以有不同用户的分组在传送，所以线路利用率较高。

2．各种交换方式的适用范围

（1）电路交换方式通常应用于公用电话网、公用电报网及电路交换公用数据网（CSPDN）等通信网络中。前两种电路交换方式是传统方式；后一种方式与公用电话网基本相似，但它

是用四线或二线方式连接用户，适用于较高速率的数据交换。正由于它是专用的公用数据网，所以其接通率、工作速率、用户线距离、线路均衡条件等均优于公用电话网，其优点是实时性强、延迟很小、交换成本较低；其缺点是线路利用率低。电路交换适用于一次接续后、长报文的通信。

（2）报文交换方式适用于实现不同速率、不同协议、不同代码终端的终端之间或一点对多点的以报文为单位进行存储一转发的数据通信。由于这种方式的网络传输时延大，并且占用了大量的内存与外存空间，所以不适用于要求系统安全性高、网络时延较小的数据通信。

（3）分组交换是在存储—转发方式的基础上发展起来的，但它兼有电路交换及报文交换的优点。它适用于对话式的计算机通信，如数据库检索、图文信息存取、电子邮件传递和计算机间通信等各方面，其优点是传输质量高、成本较低，并可在不同速率的终端之间通信；其缺点是不适宜于实时性要求高、信息量很大的业务使用。

本 章 小 结

本章主要讲述了以下内容。

（1）计算机网络的产生与发展分为 4 个阶段。第一代计算机网络是以单个计算机为中心的远程联机系统；第二代计算机网络是以多个主机通过通信线路互连起来，为用户提供服务的系统；第三代计算机网络是具有统一的网络体系结构并遵循国际标准的开放式和标准化的网络；第四代计算机网络是以 Internet 为代表的高速互联网。

（2）计算机网络是把分布在不同地点且具有独立功能的多个计算机，通过通信设备和线路连接起来，在功能完善的网络软件运行下，以实现网络中资源共享为目标的系统，具有数据通信、资源共享、分布式处理等功能。

（3）计算机网络体系结构是指整个网络系统的逻辑组成和功能分配，它定义和描述了一组用于计算机及其通信设施之间互连的标准和规范的集合，是使这个计算机网络及其部件所应该完成的功能的精确定义。最重要的计算机网络体系结构标准是 OSI 与 TCP/IP。

（4）数据通信是通信技术和计算机技术相结合而产生的一种新的通信方式。数据通信的任务是以可靠高效的手段来传输信号，涉及的内容包括信号传输、传输媒体、信号编码、接口、数据链路控制以及信道复用。数据通信技术是计算机网络通信技术的支撑技术，它依照通信协议，利用数据传输技术在两个功能单元之间传递数据信息，它可实现计算机与计算机、计算机与终端、终端与终端之间的数据信息传递。

思 考 题

一、填空题

1．Internet 的前身是_____。

2．_____是计算机网络的主要功能之一，用来在计算机系统之间传送各种信息。

3．OSI 参考模型采用____的概念，具有很高的互通性和互操作性。

4．数据链路层完成的是网络中相邻节点之间 _____ 数据通信。

5．TCP/IP 体系结构可分为 4 层，由低到高依次为：_____ 、_____ 、_____ 、_____ 。

二、选择题

1．关于计算机网络的产生和发展，下列说法中，_____ 是错误的。

A．计算机网络的产生和发展是现代社会发展的必然结果

B．计算机网络是计算机技术和通信技术相结合的产物

C．计算机网络的发展几乎与计算机的发展一同起步

D．计算机技术和通信技术的首次结合是计算机网络发展的一个里程碑

2．下列哪一个选项既符合网络的建设目的和组成，又与网络本质相符的计算机网络定义是_____ 。

A．在网络协议控制下，由多台主计算机、若干台终端、数据传输设备组成计算机复合系统

B．凡将地理位置不同、具有独立功能的多个计算机系统通过通信设备和线路连接起来，以功能完善的网络软件实现网络中资源共享的系统

C．以相互共享资源方式而连接起来，并且各自具有独立功能的计算机系统的集合

D．计算机系统与通信系统的结合在一起形成的系统

3．关于计算机网络硬件组成的终端，错误的说法是_____ 。

A．终端有近程和远程之分

B．终端不能直接连接到主机上

C．终端一般是使用性能较差的计算机

D．远程终端一般连接在通信控制处理机上

4．网络中的主机指的是_____ 。

A．主要的计算机

B．承担数据处理的计算机

C．进行数据处理的单机

D．进行数据处理的多机系统

5．_____ 不是通信子网的功能。

A．数据传输　　B．数据转接　　C．数据采集　　D．数据交换

6．计算机网络的双子网指的是通信子网和_____ 。

A．软件子网　　B．资源子网　　C．媒体子网　　D．硬件子网

7．关于计算机网络的功能，正确的说法是_____ 。

A．电子邮件的内容只能是纯文本

B．计算机网络所提供的综合信息服务功能不包括视频信息

C．计算机网络已经称为信息社会中传送与处理信息的惟一手段

D．计算机网络具有维护方便、扩展灵活的功能

8．下列关于星形拓扑的说法中，不正确的是_____ 。

A．是一种集中控制的主从式网络结构　　B．增加节点比较容易

C．节点间的通信都要通过中心节点　　D．网络的可靠性高

第 2 章　计算机网络硬件基础

本章要点

数据线的分类与制作、常用的计算机网络硬件的概念、分类、功能和特点、安装和配置等。

- **本章目标**
- 了解数据线的分类，重点掌握双绞线的分类与制作
- 理解网卡的概念、分类、安装和选购
- 理解服务器的概念、分类、特点
- 理解集线器的概念、分类、安装和选购
- 了解交换机的工作原理、特性、分类
- 了解路由器的硬件基本组成和简单的工作原理

2.1　数据线的分类与制作

2.1.1　双绞线及制作

1．双绞线

双绞线的价格低廉、连接可靠、维护简单，可提供高达 1000Mbps 的传输带宽，不仅可用于数据传输，而且还可以用于语音和多媒体传输。目前的超五类和六类非屏蔽双绞线可以轻松提供 155Mbps 的通信带宽，并拥有升级至千兆的带宽潜力，因此，成为当今水平布线的首选线缆。

双绞线是由不同颜色的 4 对 8 芯线组成，每两条按一定规则绞，成一个芯线对，作为以太局域网最基本的连接、传输介质。

双绞线一般有屏蔽（Shielded Twisted-Pair，STP）与非屏蔽（Unshielded Twisted-Pair，UTP）双绞线之分，有屏蔽当然在电磁屏蔽性能方面比非屏蔽要好，但价格也贵。

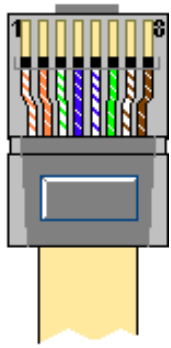
双绞线按电气性能通常分为三类、四类、五类、超五类、六类、七类双绞线等类型，数字越大，版本越新、技术越先进、带宽也越宽。三类、四类线目前在市场上几乎已消失。目前，在一般局域网中常见的是五类、超五类或者六类非屏蔽双绞线。屏蔽的五类双绞线外面包有一层屏蔽用的金属膜，它的抗干扰性能好，但应用的条件比较苛刻。并非采用了屏蔽的双绞线，在抗干扰方面就一定强于非屏蔽双绞线。屏蔽双绞线的屏蔽作用只在整个电缆均有屏蔽装置且两端正确接地的情况下才能发挥。因此，要求整个系统（包括电缆、插座、水晶头和配线架等）全部是屏蔽器件，同时建筑物需要有良好的地线系统。事实上，在实际施工时，很难全部完美接地，从而使屏蔽层本身成为最大的干扰源，导致性能甚至远不如非屏蔽双绞线 UTP。除非有特殊需要，通常在综合布线系统中只采用非屏蔽双绞线。双绞线的结构

如图 2.1（a）所示。

2．RJ-45 水晶头

双绞线的两端必须都安装如图 2.1(b)所示的 RJ-45 水晶头，以便插在网卡、集线器(Hub)或交换机（Switch）RJ-45 接口上。RJ-45 水晶头虽小，但不能小看它在网络上的重要性，在许多网络故障中就有相当一部分是因为水晶头质量不好而造成的。

（a）双绞线的结构



（b）RJ-45 水晶头

图 2.1　双绞线的结构和 RJ-45 水晶头

3．双绞线网线的制作工具

在双绞网线制作中，最简单的方法是只需一把网线钳，它可以完成剪线、剥线和压线三种用途。在购买网线钳时一定要注意选对种类，因为网线钳针对不同的线材会有不同的规格，一定要选用双绞线专用的网线钳来制作网线。

4．双绞线网线的制作

因为双绞线网线的制作非常简单，就是把双绞线的 4 对 8 芯网线按一定规则插入到水晶头中，所以这类网线的制作所需材料只是双绞线和水晶头；所需工具也较简单，通常仅需一把专用网线钳。双绞线网线的制作其实就是网线水晶头的制作。

1）直通RJ-45 接头的制作

这是一种最常用的网线制作规则。所谓直通 RJ-45 接头接法，是指它能满足 EIA/TIA568 标准，具体是：第 1 脚——橙白、第 2 脚——橙色、第 3 脚——绿白、第 4 脚——蓝色、第 5 脚——蓝白、第 6 脚——绿色、第 7 脚——棕白、第 8 脚——棕色。

这种接线方法也应用于集线器（交换机）与工作站计算机之间的连接，也是“直连线”所应用的范围。

2）1—3、2—6 交叉接法

虽然双绞线有 4 对 8 条芯线，但实际上在网络中只用到了其中的 4 条，即水晶头的第 1 脚、第 2 脚、第 3 脚、第 6 脚，它们分别起着收、发信号的作用。这种交叉网线的芯线排列规则是：网线一端的第 1 脚连接另一端的第 3 脚，网线一端的第 2 脚连接另一端的第 6 脚，其他脚一一对应即可。这种排列做出来的通常称之为“交叉线”。

这种网线一般用在集线器（交换机）的级连、服务器与集线器（交换机）的连接、对等网计算机的直接连接等情况下。

两端都做好水晶头后，即可用网线测试仪进行测试。如果测试仪上的 8 个指示灯都依次为绿色闪过，则证明网线制作成功。

2.1.2 光纤

光纤即光导纤维，是一种细小、柔韧并能传输光信号的介质。光纤组成如图 2.2 所示。光缆由多条光纤组成。与双绞线和同轴电缆相比，光缆适应了目前网络对长距离传输大容量信息的要求，在计算机网络中发挥着十分重要的作用。

图 2.2 光纤组成

最基本的光纤通信系统由数据源、光发送机和调制器、光学信道、光接收机组成。其中，数据源包括所有的信号源，它们是话音、图像、数据等业务经过信源编码所得到的信号；光发送机和调制器则负责将信号转变成适合在光纤上传输的光信号。光学信道包括最基本的光纤，还有中继放大器 EDFA 等；而光学接收机则接收光信号，并从中提取信息，然后转变成电信号，最后得到对应的话音、图像、数据等信息。光通信系统如图 2.3 所示。

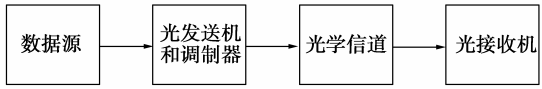


图 2.3 光通信系统图

光纤通信的最主要的优点是：

（1）容量大。因光纤工作频率比目前电缆使用的工作频率高出 8～9 个数量级，故所开发的容量很大。

（2）衰减小。光纤的每公里衰减比目前容量最大的通信同轴电缆的每公里衰减要低一个数量级以上。

（3）体积小，重量轻，同时有利于施工和运输。

（4）防干扰性能好。光纤不受强电干扰、电气化铁道干扰和雷电干扰，抗电磁脉冲能力也很强，保密性好。

（5）节约有色金属。一般通信电缆要耗用大量的铜、铝或铅等有色金属。光纤本身是非金属，光纤通信的发展将为国家节约大量有色金属。

（6）成本低。目前市场上各种电缆金属材料的价格不断上涨，而光纤的价格却有所下降。这为光纤通信的迅速发展创造了重要的前提条件。

2.1.3 同轴电缆

同轴电缆也是局域网中最常见的传输介质之一，它主要应用于环形小型局域网中。虽然这种网络相对于双绞线星形网络来说存在诸多不足之处，但是它的优点也是非常明显的，那就是它无需任何集中接入设备，就可以同时接入多达 20 台工作站，它的网络构建成本非常低。

同轴电缆网线的制作材料及工具主要包括如下几种：同轴电缆（包括“粗缆”和“细缆”两种）、中继器、收发器（用细同轴电缆组网时没有这一项）、收发器电缆（用细同轴电缆组网时没有这一项）、粗同轴电缆网线附件（N 系列接头、N 系列终端匹配器、N 系列端接器）、细同轴电缆附件（BNC 电缆连接器、BNC T 型接头、BNC 桶型接头、BNC 终端匹配器）、同

轴电缆网线压线钳等。

同轴电缆以太网连接的传输介质就是采用同轴电缆，常见的有线电视电缆大同小异。应用于计算机网络的同轴电缆主要有两种，即“粗缆”和“细缆”，都属于“基带同轴电缆”（以区别于广播电视所用的“宽带同轴电缆”）。

同轴电缆以硬铜线为芯，外包一层绝缘材料。这层绝缘材料用密织的网状导体环绕，网外又覆盖一层保护性材料。计算机网络一般选用 RG-8 规格的以太网粗缆和 RG-58 规格的以太网细缆，它们的匹配阻抗均为 50Ω。

粗缆的全称为“粗同轴电缆”，简称为“AUI”。细缆的全称为“细同轴电缆”，简称为“BNC”。细同轴电缆与粗同轴电缆的结构类似，只是直径小一些。

粗同轴电缆与细同轴电缆取决于同轴电缆的直径大小。粗缆适用于比较大型的局部网，它的标准距离长、可靠性高。由于安装时不需要切断电缆，因此可以根据需要灵活调整计算机的入网位置。因为粗缆网络必须安装收发器和收发器电缆，安装难度大，单价也较细缆贵许多，所以总体造价高。相反，细缆安装则比较简单，造价也较低。由于安装过程要切断电缆，两头必须装上基本网络连接头（BNC），然后接在 T 型连接器两端，所以当接头多时容易产生接触不良的隐患，这也是目前以太网所发生的最常见故障之一。

目前，同轴电缆在企业网络中的应用已经不多见了。

2.2 网卡

2.2.1 网卡的概念

网卡即网络适配器，又称 NIC，是将若干计算机连接成一个网络系统不可缺少的硬件设备之一。

网卡的基本功能是：实现工作站与局域网传输介质之间的物理连接和电信号匹配，接收和执行工作站与服务器送来的各种控制命令，完成物理层的功能。

每一块网卡都有全球惟一的物理地址（称为 MAC 地址）。MAC 地址是由 6 位 Byte 的数字串（共 48 位二进制）组成，数字串通常用冒号隔开，例如 00:60:8C:00:54:99。通常分为两部分：生产商 ID 和设备 ID。

（1）生产商 ID。前面 3 位 Byte（24 位二进制）代表厂商，3Com 公司为 00-60-8C，Intel 公司为 00-AA-00。有些生产厂商有几个不同的生产商 ID。

（2）设备 ID（24 位）。后面 3 位 Byte（24 位二进制）代表制造商为某具体设备分配的 ID。常见网卡如图 2.4 所示。

图 2.4 常见网卡

2.2.2 网卡的分类

随着计算机网络技术的飞速发展，为了满足各种应用环境和应用层次的需求，出现了许多不同类型的网卡，网卡的划分标准也因此出现了多样化。

1．按总线接口类型划分

1）ISA总线网卡

ISA 总线网卡是早期的一种接口类型网卡。在 20 世纪 80 年代末 90 年代初，几乎所有内置板板卡都采用 ISA 总线接口类型，直到 20 世纪 90 年代末期都还有部分这种接口类型的网卡。这种总线接口不仅用于网卡，像现在的 PCI 接口一样，当时也普遍应用于包括网卡、显卡、声卡等在内所有内置板板卡。

2）PCI总线网卡

这种总线类型的网卡是目前最主流的一种网卡接口类型。目前能在市面上买到的网卡基本上是这种总线类型的网卡。目前主流的 PCI 规范有 PCI2.0、PCI2.1 和 PCI2.2 三种，对于 PC 上用的 32 位 PCI 网卡，三种接口规范的网卡在外观上基本相同（主板上的 PCI 插槽也一样），服务器上用的 64 位 PCI 网卡在外观上与 32 位的有较大差别，主要体现在金手指的长度较长。

3）PCI-X总线网卡

这是目前一种在服务器上使用的网卡类型，它与原来的 PCI 相比，在 I/O 速度方面提高了 1 倍，比 PCI 接口具有更快的数据传输速度（2.0 版本最高可达到 266MB/s 的传输速率）。目前，这种总线类型的网卡在市面上还很少见，主要是由服务器生产厂商随机独家提供，如在 IBM 的 X 系列服务器中可以见到它的踪影。PCI-X 总线接口的网卡一般采用 32 位总线宽度，有的也采用 64 位数据宽度。

4）PCMCIA总线网卡

这种类型的网卡是笔记本电脑专用的，它受笔记本电脑的空间限制，体积远不可能像 PCI 接口网卡那么大。随着笔记本电脑的日益普及，这种总线类型的网卡目前在市面上较为常见，很容易找到，而且现在生产这种总线型的网卡的厂商也较原来多了许多。

5）USB接口网卡

USB（Universal Serial Bus，通用串行总线）已经被广泛应用于鼠标、键盘、打印机、扫描仪、MODEM、音箱等各种设备。由于其传输速率远远大于传统的并行口和串行口，设备安装简单且支持热插拔。USB 设备一旦接入，不必重新启动系统就可立即投入使用。当不再需要某台设备时，可以随时将其拔除，并可再在该端口上插入另一台新的设备。USB 接口网卡也用得越来越多。

2．按网络接口类型划分

除了可以按网卡的总线接口类型划分外，还可以按网卡的网络接口类型来划分。因为网卡最终要与网络进行连接，所以必须有一个接口使网线通过它与其他计算机网络设备连接起来。不同的网络接口适用于不同的网络类型，目前常见的接口主要有以太网的 RJ-45 接口、细同轴电缆的 BNC 接口和粗同轴电缆的 AUI 接口、FDDI 接口、ATM 接口等。而且，有的网卡为了适用于更广泛的应用环境，提供了两种或多种类型的接口，如有的网卡会同时提供 RJ-45 接口、BNC 接口或 AUI 接口。

1）RJ-45 接口网卡

这是最为常见的一种网卡，也是应用最广的一种接口类型网卡，这主要得益于双绞线以

太网应用的普及。因为这种 RJ-45 接口网卡就是应用于以双绞线为传输介质的以太网中。

2）BNC接口网卡

这种接口网卡应用于以细同轴电缆作为传输介质的以太网或令牌网中，目前这种类型的接口网卡较少见，主要因为以细同轴电缆作为传输介质的网络比较少。

3）AUI接口网卡

这种类型的接口网卡应用于以粗同轴电缆作为传输介质的以太网或令牌网中，这种类型的接口网卡目前很少见，因为以粗同轴电缆作为传输介质的网络很少。

4）FDDI接口网卡

这种接口网卡适应于 FDDI 网络中，这种网络具有 100Mbps 的带宽，因为它所使用的传输介质是光纤，所以这种 FDDI 接口网卡的接口也是光模接口。随着快速以太网的出现，它的速度优越性已不复存在，因它必须采用昂贵的光纤作为传输介质的缺点并没有改变，所以目前也非常少见。

5）ATM接口网卡

这种类型的接口网卡应用于 ATM 光纤（或双绞线）网络中。它能提供物理的传输速率达 155Mb/s。

3．按带宽划分

随着网络技术的发展，网络带宽也在不断提高，但是不同带宽的网卡所应用的环境也有所不同，价格也完全不同，为此有必要对网卡的带宽做进一步介绍。

目前主流的网卡主要有 10Mbps 网卡、100Mbps 以太网卡、10Mbps/100Mbps 自适应网卡、1000Mbps 以太网卡四种。

1）10Mbps网卡

10Mbps 网卡是一种低档网卡。它的带宽限制在 10Mbps，这在当时的 ISA 总线类型的网卡中较为常见，目前 PCI 总线接口类型的网卡中也有一些是 10Mbps 网卡，不过目前这种网卡已不是主流。这类带宽的网卡仅适用于一些小型局域网或家庭需求，中型以上网络一般不选用。

2）100Mbps网卡

100Mbps 网卡在目前来说是一种技术比较先进的网卡，它的传输 I/O 带宽可达到 100Mbps，这种网卡一般用于骨干网络中。目前这种带宽的网卡在市面上已逐渐得到普及。

3）10Mbps/100Mbps 自适应网卡

这是一种能自适应 10Mbps 和 100Mbps 两种带宽的网卡，也是目前应用最为普及的一种网卡类型，因为它能自动适应两种不同带宽的网络需求，所以保护了用户的网络投资。因为它既可以与老式的 10Mbps 网络设备相连，又可应用于较新的 100Mbps 网络设备连接，所以得到了用户的普遍认同。这种带宽的网卡会自动根据所用环境选择适当的带宽，如果与老式的 10Mbps 旧设备相连，则它的带宽就是 10Mbps；如果与 100Mbps 网络设备相连，则它的带宽就是 100Mbps，它能兼容 10Mbps 的老式网络设备和新的 100Mbps 网络设备。

4）1000Mbps以太网卡

1000Mbps 以太网（Gigabit Ethernet）是一种高速局域网技术，它能够在铜线上提供 1Gbps 的带宽。与它对应的网卡是千兆网卡，这类网卡的带宽也可达到 1Gbps。千兆网卡的网络接口有两种主要类型：一种是普通的双绞线 RJ-45 接口，另一种是多模 SC 型标准光纤接口。

4．按网卡应用领域划分

如果根据网卡所应用的计算机类型划分，可以将网卡分为应用于工作站的网卡和应用于服务器的网卡。前面介绍的基本上都是工作站网卡，其实通常也应用于普通的服务器上。但是在大型网络中，服务器通常采用专门的网卡。它相对于工作站所用的普通网卡来说，在带宽（通常在 100Mbps 以上，主流的服务器网卡都为 64 位千兆网卡）、接口数量、稳定性、纠错等方面都有比较明显的提高。有的服务器网卡还支持冗余备份、热插拔等服务器专用功能。

2.2.3 网卡的安装

1．驱动程序的安装

虽然安装了网卡，但如果不进行驱动程序的安装与系统的配置，则不能起到网络连接的作用。不过，随着微软 Windows 系统对硬件支持范围的扩大，许多网卡的驱动程序都已内置，从而不需要另外提供网卡的厂家驱动程序，当系统进入后即可检测到硬件，然后安装 Windows 系统自带的驱动程序，真正实现“即插即用”。但是，为了实现网卡的真正性能，如果有网卡厂家的驱动程序，建议还是安装厂家提供的驱动程序；如果没有，就可以使用 Windows 系统自带的驱动程序，网卡也可正常工作；如果 Windows 系统没有提供此型号网卡的驱动程序，则一定要安装厂家的驱动程序或者选择一个兼容该型号网卡的其他型号驱动程序。

为了掌握网卡驱动程序的安装方法，下面介绍在 Windows 98 系统中安装网卡驱动程序的方法。

第 1 步：在“控制面板”中双击“添加新硬件”选项，出现“添加新硬件向导”对话框。

第 2 步：单击“下一步”按钮，出现对话框提示用户系统将对新添加的硬件进行搜索。

第 3 步：选择第一个单选项，单击“下一步”按钮，出现的对话框中显示了搜索驱动程序的多种定位方法，根据实际选择一项或多项复选项。

选择好驱动程序的位置后，单击“下一步”按钮或“确定”按钮后即可自动完成驱动的安装。安装完后，系统提示要求重新启动系统，重启后生效。

2．网卡的配置

网卡的配置是整个对等网组建成功与否的关键，在网卡的配置中需要做以下几个方面的配置：

（1）安装网络客户。

（2）安装网络协议。

（3）配置工作组。

（4）配置客户机网卡的 IP 地址。

通常在安装网卡后，基本的网络组件，如网络客户、TCP/IP 协议都已安装，只需进行一些必要的配置即可。下面介绍在网卡安装后需要对系统未自动完成的部分做的工作。

第 1 步：在“控制面板”中双击“网络”选项，出现“网络属性”对话框（如果在桌面上已有“网上邻居”项，也可直接在其上单击鼠标右键，然后选择“属性”选项，同样可打开这个“网络属性”对话框）。

第 2 步：因为要在 Windows 98 对等网中实现打印共享之类的网络任务，仍需使用 NetBEUI 协议，所以除了系统自动安装的 TCP/IP 协议外，还需添加这个协议（在 Windows ME/2000/XP 等系统中不需要）。安装的方法很简单，单击“添加”按钮。

第 3 步：选择“协议”项，然后单击“添加”按钮，在出现的对话框的左栏中选择“Microsoft”

选项，在右边列表中双击“NetBEUI”选项。

第 4 步：添加 NetBEUI 协议后，不要急于重新启动系统，为了完成对等资源的共享安装，要把文件及打印的共享服务程序加进去。方法与添加 NetBEUI 协议类似，不同的是选择的不是“协议”，而是“服务”，然后在对话框中双击“Microsoft 网络上的文件与打印机共享”选项。添加这个服务项后，对等网中的用户才可以通过网络进行文件和打印机共享。

第 5 步：安装协议和服务后，就要配置客户机网卡的 IP 地址。选择对应网卡的 TCP/IP 项（注意：不是选择物理的网卡项），然后单击“属性”按钮，打开网卡的 TCP/IP 属性配置对话框。

第 6 步：因为在对等网中没有专门的 DHCP 服务器来为各客户机自动选择 IP 地址，所以需要选择“指定 IP 地址”单选项，然后在下面的“IP 地址”和“子网掩码”栏中分别输入一个 IP 地址和子网掩码。

第 7 步：单击“标志”标签项，为计算机配置网络中惟一的计算机名，并配置网络的工作组名。配置好后单击“确定”按钮生效。

设置好后所有选项后，单击“确定”按钮，系统即进行自动更新，完成后即要求重新启动系统，重启后即生效。

2.2.4 网卡的选购

网卡看似一个简单的网络设备，但它的作用却是决定性的。加上目前网卡品牌、规格繁多，稍不留意，很可能购买的网卡不能配套使用或者质量太差。如果网卡性能不好，即使其他网络设备的性能再好，也无法实现用户预期的效果。在选购网卡时，要注意以下方面。

1．网卡的材质和制作工艺

网卡的制作工艺主要体现在焊接质量、板面光洁度和网卡的板材上。网卡所采用的晶振也很重要。好的网卡通常采用高精度的 SKO25MHz 的晶振，以便可靠保证数据传输的精确同步性，大大减少丢包的可能性。在线路的设计上应尽量使晶振靠近主芯片，使信号走线的长度大大缩短，可靠性进一步增加。

2．选择恰当的品牌

如果是为较大型的企业网络购买网卡，建议最好购买信誉较好的名牌产品，如 3COM、Intel、D-Link、Accton 等。国产较好信誉的品牌也是不错的选择，如实达、TP-Link、D-Link 等。

3．根据网络类型选择网卡

由于网卡种类繁多，不同类型的网卡的使用环境是不一样的。因此，在选购网卡之前，应明确所选购网卡使用的网络及传输介质类型、与之相连的网络设备带宽等情况。目前市场上的网卡根据连接介质的不同，基本上可以分为粗缆网卡（AUI 接口）、细缆网卡（BNC 接口）及双绞线网卡（RJ-45 接口）。如果是以双绞线作为传输介质，则要选用 RJ-45 接口网卡；如果传输介质是细同轴电缆的，则要选用 BNC 接口网卡；如果是采用粗同轴电缆，则要选用 AUI 接口网卡。

4．根据计算机插槽总线类型选购网卡

由于网卡是要插在计算机的插槽中的，所以要求所购买的网卡总线类型必须与装入机器的总线相符。总线的性能直接决定从服务器内存和硬盘向网卡传递信息的效率。与 CPU 一样，影响硬件总线性能的因素也有两个：数据总线的宽度和时钟速度。网卡按总线类型，可以分为 PCI 网卡、ISA 网卡、EISA 网卡及服务器 PCI-X 总线网卡。目前主流网卡是 PCI 网卡。

5．根据使用环境选择网卡

为了使选择的网卡与计算机协同高效地工作，必须根据使用环境来选择合适的网卡。例如，若购买了一个价格昂贵、功能强大、速度快捷的网卡，却安装到一台普通的工作站中，则大材小用，给资源造成了很大的浪费和闲置。相反，如果在一台服务器中安装一个性能普通、传输速度低的网卡，则很容易产生瓶颈现象，从而抑制整个网络系统的性能发挥。因此，在选用时一定要注意应用环境，比如服务器端网卡由于技术先进，价钱会贵很多，为了减少主 CPU 占有率，应选择带有高级容错、带宽汇聚等功能的服务器网卡，从而使服务器通过增插几个网卡来提高系统的可靠性。

2.3 服务器概述

2.3.1 服务器的主要性能特点

服务器其实也是一种计算机，它是由 PC（个人计算机）发展而来的。在早期，网络不是很普及，并没有服务器这个名称，当时，在整个计算机领域中只有大型计算机和微型计算机两大类。随着网络（特别是局域网）的发展和普及，“服务器”这个中间层次的计算机开始得到业界的认同，并随着网络的普及和发展不断得到发展。尽管如此，服务器与普通的计算机又不完全一样，它有特殊性要求，即服务器的四大主要性能特点：可靠性、可用性、可扩展性和可管理性。

（1）作为一台服务器，首先要求的是它必须具有可靠性。因为服务器面对的是整个网络的用户，而不是本机登录用户，只要网络中有用户使用，服务器就不能中断工作。在一些特殊应用领域，即使无用户使用，有些服务器也必须不间断地工作，因为它必须持续地为用户提供连接服务，这就是服务器首先必须具备极高的可靠性的根本原因。

（2）服务器要为众多用户提供服务，不具有高的连接和运算性能是无法承受的，这是指服务器的可用性。

（3）服务器还必须具有可扩展性，因为网络不可能长久不变，如果不具有可扩展性，当用户增多时就不能胜任，一台几万元甚至几十万元的服务器在短时间内就要遭到淘汰，这是许多企业都无法接受的。为了保持高的可扩展性，通常需要服务器具备可扩展空间和冗余件（如磁盘矩阵位、PCI 和内存条插槽位等）。

（4）服务器必须具备自动报警功能，并配有相应的备份、在线诊断和恢复系统，以便在出现故障时能及时能恢复服务器的运作，这就是可管理性。

2.3.2 服务器的主要外观特点

服务器的外观如图 2.5 所示。

1．机箱大

从外观结构上看，服务器的机箱一般比较大，有的虽然外观上看似与普通 PC 差不多，但实际上还是要大些，即使是入门级的 PC 服务器也都有比 PC 更大的机箱。对于一些中、高档的专业服务器，机箱的差别就更大。

服务器的机箱大是有理由的。因为服务器需要安装、连接的设备多，需占用较大空间，同时还需要一些备用设备安置位，如磁带机、磁盘阵列、多 PCI 或 PCI-X 插卡等需要占用空

间。服务器通常要与许多设备进行连接，如在服务器主板或专用板卡上要插装许多适配器卡，有的还要安装几个可热插拔的硬盘和电源（俗称“备份电源”），一般还安装供系统备份和恢复用的磁带机。另外，由于安装、连接的设备多，工作时发热量也非常大，必须有足够的空间来散热，以确保服务器能长时间稳定工作。以上这些都决定了服务器的机箱必须比普通 PC 大，即使是 DIY PC 服务器，为了保证服务器长期稳定工作，也必须加大机箱，在选购或配置 PC 服务器时必须加以注意。

图 2.5　服务器的外观

2．硬盘、内存容量大

服务器要面对众多的用户，接受所有用户的请求，而且还必须安装、保存许多大容量的服务器专用系统、软件以及其他一些数据库文件，这都要求服务器的硬盘容量要足够大。以前因为硬盘容量比较小（早期的才几百兆），所以通常采取磁盘矩阵，在服务器的磁盘架上并列安装许多磁盘，虽然这不仅是用于提高整个服务器磁盘容量，但这在当时也是提高磁盘容量的主要目的之一。目前的硬盘容量非常大，最高可达 200GB 以上。目前，一般的中、小企业网络服务器，在容量上只需一块硬盘就足够了，采用磁盘矩阵的主要目的是提高磁盘存取性能和安全恢复性能。

3．主板大

一般来说，服务器主板要比 PC 主板大许多，这主要是因为在服务器中要安装比 PC 多许多的组件，如更多的 PCI（5 条以上）、PCI-X、内存插槽（4 条以上），还可能安装多个 CPU 插座。有的服务器为了节省主板的空间，把部分比较集中的功能件由另外一块单独的板卡提供，如有的服务器把所有 PCI 或 PCI-X 插槽集中在一块板上并放置在机箱外面的一个单独盒子中，然后通过一条数据电缆与主板进行连接。

4．有备份部件

在一些较高档的服务器中，可以看到在一台机中有两个电源、两个风扇，还装有一些并没有真正连接的网卡和未使用的硬盘。它们都是用于当正在工作的相同部件出现故障时接替它们工作的，俗称“备份部件”或“冗余件”。有了这些备份件，即使工作部件出现了故障（有的甚至是当工作部件未出现正式故障前，由系统发现一些不正常预兆后立即替换），也不会造成服务器停止工作，使整个网络保持持续正常运行。这对确保服务器的高稳定、不间断工作非常重要。电源、风扇和网卡备份可能令人容易理解，直接替换即可。对于硬盘备份，一般来说，用于备份的硬盘要定期地对正在工作的硬盘进行备份，以便使备份硬盘在接替故障硬盘后可以立即为当前最新的网络系统配置提供服务。

5．支持热插拔

因为采用“热插拔”技术的设备通常比较贵，所以在 PC 中就不具备这项特性。热插拔技术主要是方便对服务器的维护（这也是服务器所必需的）。例如，发现硬盘不够容量或者发现某个硬盘损坏时，如果硬盘支持热插拔，则只需把新的硬盘插入服务器预留的位置，或者把坏的硬盘从服务器直接拔下来进行维修，这一切操作都不需要关闭服务器系统，这样就保证了服务器的不间断运行。目前主要支持热插拔技术的有硬盘、电源、风扇、PCI 适配卡（主要是指网卡）等。目前，还有一些较高档的服务器支持内存、CPU 的热插拔。凡是支持热插拔技术的都可以在线（不关闭服务器电源）的情况下直接插上新的部件或者从服务器上拔下

旧的部件，这样极大地方便了服务器的维护，确保服务器恒久运行。

2.3.3 服务器的分类

按应用层次划分是服务器最为普遍的一种划分方法，它主要根据服务器在网络中应用的层次（或服务器的档次）来划分。按这种划分方法，服务器可分为入门级服务器、工作组级服务器、部门级服务器、企业级服务器。

1．入门级服务器

这类服务器是最基础的一类服务器，也是最低档的服务器。随着 PC 技术的日益提高，现在许多入门级服务器与 PC 的配置差不多，所以目前也有部分人认为入门级服务器与“PC 服务器”等同。

这类服务器通常只具备以下特性：

（1）具有一些基本硬件（如硬盘、电源、风扇等）的备份，但不是必需的。

（2）采用 SCSI 接口硬盘，也可采用 SATA 串行接口。

（3）部分部件支持热插拔，如硬盘和内存等，但也不是必需的。

（4）通常只有一个 CPU，但不是绝对的，如有的 SUN 入门级服务器可支持 2 个处理器。

（5）内存容量一般在 1GB 以内，但通常会采用带 ECC 纠错技术的服务器专用内存。

这类服务器主要采用 Windows 或者 NetWare 网络操作系统，可以充分满足办公室型的中、小型网络用户的文件共享、数据处理、Internet 接入及简单数据库应用的需求。这种服务器与一般的 PC 很相似，有很多小型公司干脆就用一台高性能的品牌 PC 作为服务器，这种服务器无论是在性能上还是在价格上都与一台高性能的品牌 PC 相差无几。

入门级服务器所连接的终端比较有限（通常为 20 台左右），并且稳定性、可扩展性以及容错冗余性能较差，仅适用于无大型数据库数据交换、日常工作网络流量不大、无需长期不间断开机的小型企业。这种服务器一般采用 Intel 的专用服务器 CPU 芯片，基于 Intel 架构（又称“IA 结构”）。

2．工作组级服务器

工作组级服务器是一个比入门级服务器高一个层次的服务器，但仍属于低档服务器之类。从名字也可以看出，它只能连接一个工作组（50 台左右）的用户，网络规模较小，服务器的稳定性也不像企业级服务器那样高，在其他性能方面的要求也相应要低一些。工作组级服务器具有以下主要特点：

（1）通常仅支持单或双 CPU 结构的应用服务器。

（2）可支持大容量的 ECC 内存和增强服务器管理功能的 SM 总线。

（3）功能较全面、可管理性强，易于维护。

（4）采用 Intel 服务器 CPU 和 Windows/NetWare 网络操作系统，但也有一部分是采用 UNIX 系列操作系统的。

（5）可以满足中、小型网络用户的数据处理、文件共享、Internet 接入及简单数据库应用的需求。

工作组级服务器与入门级服务器相比，性能有所提高，功能有所增强，有一定的可扩展性，但容错和冗余性能仍不完善，也不能满足大型数据库系统的应用。

3．部门级服务器

这类服务器属于中档服务器之列，一般都是支持双 CPU 以上的对称处理器结构，具备比较完全的硬件配置，如磁盘阵列、存储托架等。部门级服务器的最大特点是，除了具有工作组级服务器的全部特点外，还集成了大量的监测及管理电路，具有全面的服务器管理能力，可监测温度、电压、风扇、机箱等状态参数，结合标准服务器管理软件，使管理人员能及时了解服务器的工作状况。同时，大多数部门级服务器具有优良的系统扩展性，使用户在业务量迅速增大时能够及时在线升级系统，充分保护了用户的投资。它是企业网络中分散的各基层数据采集单位与最高层的数据中心保持顺利连通的必要环节，一般为中型企业的首选，也可用于金融、邮电等行业。

部门级服务器一般采用 IBM、SUN 和 HP 各自开发的 CPU 芯片，这类芯片一般是 RISC 结构，所采用的操作系统一般是 UNIX 系列操作系统，Linux 现在也在部门级服务器中得到了广泛应用。以前能生产部门级服务器的厂商只有 IBM、HP、SUN、COMPAQ（现在也已并入 HP），随着其他一些服务器厂商开发技术的提高，现在能开发、生产部门级服务器的厂商日益增多。国内的联想、曙光、浪潮等也具备这种实力。

部门级服务器可连接 100 个左右的计算机用户、适用于对处理速度和系统可靠性高一些的中、小型企业网络，其硬件配置相对较高，其可靠性比工作组级服务器要高一些，其价格也较高（通常为 5 台左右高性能 PC 的价格总和）。由于这类服务器需要安装比较多的部件，所以机箱通常较大，一般采用机柜式结构。

4．企业级服务器

企业级服务器属于高档服务器之列。企业级服务器至少采用 4 个以上（有的高达几十个）CPU 的对称处理器结构，一般具有独立的双 PCI 通道和内存扩展板设计，具有高内存带宽、大容量热插拔硬盘和热插拔电源、超强的数据处理能力和群集性能等。企业级服务器的机箱更大，一般为机柜式结构，有的还由几个机柜来组成，像大型机一样。

企业级服务器除了具有部门级服务器的全部特性外，最大的特点是，它还具有高度的容错能力、优良的扩展性能、故障预报警功能、在线诊断和 RAM、PCI、CPU 等热插拔性能。有的企业级服务器（如 IBM 和 SUN 公司的企业级服务器）还引入了大型计算机的许多优良特性。这类服务器所采用的芯片也都是几大服务器开发、生产厂商自己开发的独有 CPU 芯片，所采用的操作系统一般也是 UNIX（Solaris）或 Linux。企业级服务器适合运行在需要处理大量数据、高处理速度和对可靠性要求极高的金融、证券、交通、邮电、通信或大型企业中。

企业级服务器适用于联网计算机在数百台以上、对处理速度和数据安全要求非常高的大型网络。企业级服务器的硬件配置最高，系统可靠性也最强。

2.4 集线器

2.4.1 集线器概述

集线器的英文是“Hub”，集线器的主要功能是对接收到的信号进行再生、整形、放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。它工作于 OSI 参考模型第二层，即“数据链路层”。

集线器是中继器的一种，其区别仅在于集线器能够提供更多的端口服务，所以集线器又

称多口中继器。集线器主要是以优化网络布线结构、简化网络管理为目标而设计的。集线器是对网络进行集中管理的最小单元，像树的主干一样，它是各分支的汇集点。

集线器常用在一个小型局域网中。集线器的一般应用如图 2.6 所示。

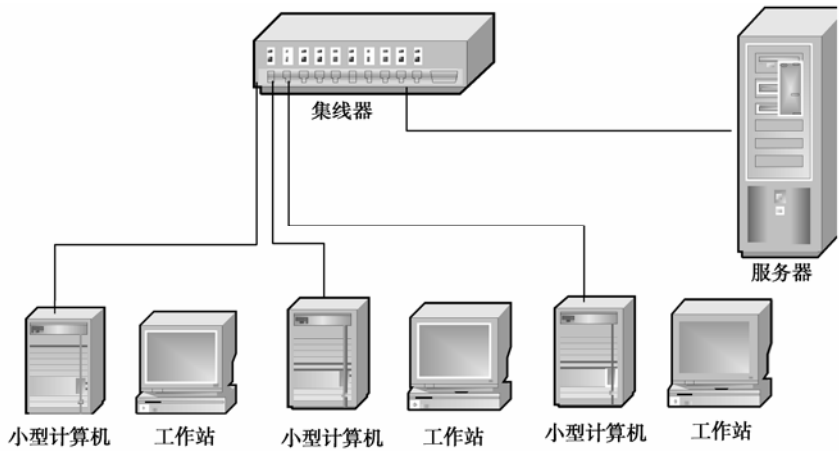


图 2.6　集线器的一般应用

以集线器为节点中心的优点是，当网络系统中某条线路或某节点出现故障时，不会影响网上其他节点的正常工作，因为它提供了多通道通信，大大提高了网络通信速度。

然而，随着网络技术的发展，集线器的缺点越来越突出，一种技术更先进的数据交换设备——交换机逐渐取代了部分集线器的高端应用。集线器的主要不足体现在以下几个方面。

1．用户带宽共享，带宽受限

集线器的每个端口没有独立的带宽，而是所有端口共享总的背板带宽，用户端口带宽较窄，并且随着集线器所连接用户的增多，用户的平均带宽不断减少，不能满足当今许多对网络带宽有严格要求的网络应用，如多媒体、流媒体应用等环境。

2．广播方式，易形成网络风暴

集线器是一个共享设备，它的主要功能只是一个信号放大和中转的设备，不具备自动寻址能力，即不具备交换作用，所有传到集线器的数据均被广播到与之相连的各个端口，容易形成网络风暴，造成网络堵塞。

3．非双工传输，网络通信效率低

在同一时刻，集线器的每一个端口只能进行一个方向的数据通信，而不能像交换机那样进行双向双工传输，网络执行效率低，不能满足较大型网络的通信需求。

因此，尽管集线器技术也在不断改进，但实质上就是加入了一些交换机技术，目前集线器与交换机的区别越来越模糊了。随着交换机价格的不断下降，仅有的价格优势已不再明显，集线器的市场越来越小，处于淘汰的边缘。尽管如此，集线器对于家庭或者小型企业来说，在经济上还是有诱惑力的，特别适用于家庭几台机的网络中。

2.4.2　集线器的分类

集线器的外观如图 2.7 所示。

集线器也像网卡一样是伴随着网络的出现而产生的，它的产生早于交换机，更早于路由器等网络设备，所以它属于一种传统的基础网络设备。集线器技术发展至今，也经历了许多

不同主流应用的历史发展时期，所以集线器产品也有许多不同类型。下面对目前的主流集线器的分类方法加以综述。

图 2.7　集线器的外观

1．按端口数划分

这是最基本的分类标准之一。按照集线器能提供的端口数划分，目前主流集线器主要有 8 口、16 口和 24 口等大类，但也有少数品牌提供非标准端口数，如 4 口和 12 口的，还有的是 5 口、9 口、18 口的集线器，这主要是想满足部分对端口数要求过严、资金投入比较谨慎的用户需求。

2．按带宽划分

按照集线器所支持的带宽不同，通常可分为 10Mbps、100Mbps、10/100Mbps 三种，基本上与网卡一样（网卡还有 1000Mbps 的，但 1000Mbps 以上带宽的一般都由交换机来提供）。这里所指的带宽是指整个集线器所能提供的总带宽，而非每个端口所能提供的带宽。在集线器中，所有端口都是共享集线器的背板带宽的，也就是说，如果集线器带宽为 10Mbps，总共有 16 个端口，若 16 个端口同时使用，则每个端口的带宽只有 10/16Mbps。连接的节点数越少，每个端口所分得的带宽就会越宽。

3．按照配置形式划分

集线器是最基础的网络设备，也是网络集中管理的最基本单元，它几乎不需要软件支持，配置起来非常简单、方便。一般情况下，只需要把节点连接好，插上电源，开启各节点即可完成连接过程的配置。按整个集线器的配置划分，一般可分为独立型集线器、模块化集线器和堆叠式集线器三种。

1）独立型集线器

这种类型的集线器在低端应用中是最多的，也是最常见的。独立型集线器是带有许多端口的单个盒子式的产品。独立型集线器之间可以用一段 10Base-5 同轴电缆把它们连接在一起，以实现扩展级联，这主要应用于总线型网络中；也可以用双绞线通过普通端口实现级联，但要注意所采用的网线跳线方式不一样，在 4.3.2 节中会具体介绍。独立型 Hub 具有低价格、容易查找故障、网络管理方便等优点，在小型的局域网中广泛使用；但这类 Hub 的工作性能比较差，尤其是在速度上缺乏优势。

2）模块化集线器

模块化集线器一般都配有机架，带有多个卡槽，每个卡槽可放一块通信卡，每个卡的作用就相当于一个独立型集线器，多块卡通过安装在机架上的通信底板进行互连并进行相互间的通信。现在常使用的模块化 Hub 一般具有 4～14 个卡槽。模块化集线器的各个端口都有专用的带宽，只在各个网段内共享带宽，网段之间采用交换技术，从而减少冲突，提高通信效率，因此又称为端口交换机模块化 Hub。其实，这类 Hub 已经采用交换机的部分技术，已不

是单纯意义上的 Hub 了，它在较大型网络中便于实施对用户的集中管理，在较大型网络中得到了广泛应用。

3）堆叠式集线器

堆叠式集线器可以将多个集线器“堆叠”使用，当它们连接在一起时，其作用就像一个模块化集线器，堆叠在一起的集线器可以作为一个单元设备来进行管理。一般情况下，当有多个 Hub 堆叠时，其中存在一个可管理 Hub，利用可管理 Hub 可对此堆叠式 Hub 中的其他“独立型 Hub”进行管理。堆叠式 Hub 可非常方便地实现对网络的扩充，是新建网络时最为理想的选择。

4．按照管理的方式分

按集线器对数据信号的管理方式划分，集线器可分为切换式、共享式和可堆叠共享式三种。

1）切换式集线器

这种集线器可以使 10Mbps 和 100Mbps 的站点用于同一网段中。一个切换式集线器重新生成每一个信号并在发送前过滤每一个包，而且只将其发送到目的地址，这与交换技术类似，也就是通常所说的智能集线器。

2）共享式集线器

这种集线器可使所有连接点的站点之间共享一个最大频宽。共享式集线器不过滤或重新生成信号，所有与之相连的站点必须以同一速度（10Mbps 或 100Mbps）工作，这是最常见的一类集线器。目前，绝大多数集线器都是这种共享式集线器，也就是说，连接在集线器上的所有节点都可共享集线器的整个带宽。

3）可堆叠共享式集线器

它可将多个集线器堆放在一起，通过特定端口互连在一起，所以也可以看成是局域网中的一个大集线器。

2.4.3 集线器的端口类型

集线器通常都提供三种类型的端口，即 RJ-45 端口、BNC 端口和 AUI 端口，以适用于连接不同类型电缆构建的网络。一些高档集线器还提供光纤端口和其他类型的端口。

1．RJ-45 端口

集线器的 RJ-45 端口既可直接连接计算机、网络打印机等终端设备，也可以与其他交换机、集线器等集线设备和路由器连接。需要注意的是，当连接至不同设备时，所使用的双绞线电缆的跳线方法有所不同。

2．BNC端口

BNC 端口是用于与细同轴电缆连接的接口。大多数 10Mbps 集线器都拥有一个 BNC 端口。当集线器同时拥有 BNC 和 RJ-45 端口时，由于既可通过 RJ-45 端口与双绞线网络连接，又可通过 BNC 端口与细缆网络连接，因此，可实现双绞线和细同轴电缆两个采用不同通信传输介质的网络之间的连接。这种双接口的特性可用于兼容原有的细同轴电缆网络（10Base-2），并可实现逐步向主流的双绞线网络（10Base-T）的过渡，还可实现与远程细同轴电缆网络（少于 185m）之间的连接。

3．AUI端口

AUI 端口可用于连接粗同轴电缆的 AUI 接头，这种端口用于与粗同轴电缆网络的连接，

目前带有这种端口的集线器比较少，只有骨干级集线器才具备。

4．集线器堆叠端口

只有堆叠式集线器才具备这种端口，它用于连接两个堆叠式集线器。一般来说，一个堆叠式集线器中同时具有两个外观类似的端口：一个标注为“UP”，另一个标注“DOWN”。在连接时，用电缆从一个集线器的“UP”端口连接到另一个堆叠式集线器的“DOWN”端口上。

2.4.4 集线器的选购要点

集线器属于基础网络设备产品，基本上不需用另外的软件提供支持，真正达到即插即用。但是，在选择集线器时，也需要考虑实际网络需求的方方面面，下面介绍集线器的选购要点。

1．带宽的选择

目前主流的集线器带宽主要有三种：10Mbps、10Mbps/100Mbps 自适应型、100Mbps。建议选择 10Mbps/100Mbps 自适应型集线器，这是因为在整个网络中或许还有一些网络设备（如网卡）不完全支持 100Mbps 的带宽，如果只选择 100Mbps 网卡很可能造成网络无法正常连通和运作。

2．端口的选择

集线器作为一个特殊的中继器，它的最大特点就是能提供多个端口，所以在端口的选择上也需要充分考虑网络的实际需要及发展需求。通过上述内容可知，集线器可以通过两种方式来获得端口的扩展：一种是通过集线器的堆叠，另一种是通过集线器的级联。这两种方法的主要应用环境有所侧重。

（1）在端口的选择上应充分考虑到网络的发展，如果仅局限于当前的网络规模，很可能会造成网络设备投资的浪费。

（2）由于连在集线器上的所有节点均争用同一个上行总线，处于同一冲突域内，所以在集线器内所连接节点数目太多，造成冲突也就可能过于频繁，因此，就要注意集线器的端口不要太多（最多不超过 16 个）。

3．网管功能选择

根据对集线器管理的方式不同可分为 Damp Hub（亚集线器）和 Intelligent Hub（智能集线器）两种。智能集线器改进了普通集线器的缺点，增加了网络的交换功能，具有网络管理和自动检测网络端口速度的能力（类似于交换机）。亚集线器只起到简单的信号放大和再生的作用，无法对网络性能进行优化。早期的大多数共享式 10Mbps 集线器一般为非智能型集线器，而现在流行的 100Mbps 集线器和 10Mbps/100Mbps 自适应集线器多为智能型集线器。

智能型集线器在目前来说是应用的主流。较大规模的网络应首选智能型集线器，这不仅是网络本身的实际需求，同时也是网络管理的需求。现在，有的智能型集线器提供网络管理功能，通过网络管理软件可以实现对集线器端口的有效管理，监控各端口的使用状况，同时也可对集线器的使用状况进行监视，及时发现和排除故障。这对于大型网络相当重要，因为这种网络的用户较多，数据流量也较大，一旦网络出现故障，如果不能及时发现、及时排除，则对整个网络的影响非常大，还有可能造成非常巨大的经济损失。由于交换机的价格不断下降，这类集线器在价格上的优势早已失去竞争力，所以这类高档集线器反而不受欢迎，人们更多选择的是交换机。

2.4.5 集线器的网络安装和连接

1．集线器的安装

集线器的安装相对简单，只要将其固定在配线柜并插上电源线即可。需要连接哪根双绞线，就把哪根双绞线的 RJ-45 头插入集线器端口即可。智能型集线器虽然也是固定好就能使用，但如果想实现远程管理，就必须进行必要的配置，为集线器指定 IP 地址信息。另外，在一些大的网络中一般都采用机架式集线器，这就涉及集线器的机架安装。

集线器从结构上来讲有机架式和桌机式两种，一般部门采用桌面式集线器，企业机房通常采用机架式集线器。机架式集线器便于固定在一个固定的地方，一般是与其他集线器、交换机、服务器安放在一个机柜中，以便于网络的连接与管理，同时也节省设备所占用的空间。如果所选购的是机架式集线器，则可以选配集线器机架（一般为厂家提供）。下面介绍机架式集线器的安装。

机架式集线器一般都是与其他设备一起安装在机柜中，这些机柜在业界都有相应的结构标准，特别是在尺寸方面有严格的规定，如宽度、1U（单元）的高度等，从而使所有设备都可以方便、美观地安装在一起。这就是集线器机箱内的部件并不多，却要一样大的原因，机箱大的另一个好处是可以更好地散热。

国际标准机柜从宽度上大致可分 19 英寸、23 英寸和 24 英寸三类，这主要是根据服务器机柜的要求而定的。根据安装设备数量的不同，还可以选择不同高度的机柜。机柜的高度通常以“U”作为单位，1U＝1.75 英寸。这种机柜的安装通常主要按以下步骤进行。

1）固定安装支架

在将集线器安装至机柜之前，应先在集线器规定位置上安装固定支架（要参照操作手册进行），这是为以后将集线器安装在机架上做准备。不同的集线器，所安装的支架有较大的差异，不过，安装原理基本上是一致的。

Cisco 公司的网络设备的尺寸大多为 19 英寸（因为 19 英寸是国际上最为流行的机柜标准）。应将 19 英寸的网络设备安装到 19 英寸机柜中；而当网络设备的尺寸为 23 或 24 英寸时，网络设备就需要安装到 23 或 24 英寸机柜中。

2）固定设备

安装支架固定好之后，把安装好支架的集线器设备放入机柜中的相应位置，并且固定在机柜中。其实这种安装方法很容易，实际上只是固定几个螺钉。

3）固定导线器

将集线器安装至机柜后，要进行网线连接。在一个机柜中，一般有几个网络设备，这样也就有许多条网线集中在这个机柜中。如果不理清楚这些网线，则会对网络管理带来非常大的不便，为此需要对网线进行捆绑安装、整理。这时，一般要为网线安装导线器，使成束的网线变得整齐和美观，并且易于管理。

在桌面上安装集线器时，可先在桌面上固定安装支架，要注意这种安装方式有两种不同的安装方向：一种是让集线器水平放置，另一种是让集线器垂直放置。

在墙面上安装集线器的方法有两种：一种是把集线器水平固定在墙上，另一种是把集线器垂直安装在墙上。

2．集线器的连接

集线器的连接很简单，基本上不需要配置。

1）集线器的信号转发原理

因为集线器采用了 CSMA/CD（载波侦听多路访问/冲突检测协议，CSMA/CD 协议为 MAC 层协议，所以集线器也含有数据链路层的内容。

10Mbps 集线器作为一种特殊的多端口中继器，它在网络中继扩展中要遵循 5-4-3 规则一个网段最多只能分 5 个子网段，一个网段最多只能有 4 个中继器，一个网段最多只能有 3 个子网段含有 PC。

集线器的工作过程是非常简单的，可以简单地描述成：首先是节点发信号到线路，集线器接收该信号，因信号在电缆传输中有衰减，集线器接收信号后将衰减的信号整形放大，最后集线器将放大的信号广播转发给其他所有端口。

2）集线器的堆叠

集线器的堆叠是通过厂家提供的一条专用连接电缆，从一台的“UP”堆叠端口直接连接到另一台集线器的“DOWN”堆叠端口。堆叠的所有集线器可视为一个整体的集线器来进行管理，也就是说，堆叠的所有集线器从拓扑结构上可视为一个集线器。这种集线器间的连接通常不会占用集线器上原有的普通端口，而且在这种堆叠端口中具有智能识别性能，所以堆叠在一起的集线器可以当做一台集线器来统一管理。集线器的堆叠技术采用了专门的管理模块和堆叠连接电缆，能够在集线器之间建立一条较宽的宽带链路，这样每个实际使用的用户带宽就有可能更宽（只有在并不是所有端口都在使用情况下）。

采用堆叠的集线器端口扩展连接方式受到集线器的种类和间隔距离的限制，首要条件是实现堆叠的集线器必须是可堆叠的；另外，因为这种堆叠连接一般彼此间隔很近（厂家所能提供的堆叠连接电缆一般是 1m 的），所以这种集线器端口扩展连接方式受距离限制太大。

3）级联

级联是另一种集线器端口扩展连接方式，是指使用集线器普通的或特定的端口来进行集线器间的连接。普通端口就是通过集线器的某一个常用端口（如 RJ-45 端口）进行连接；而特殊端口就是集线器为级联专门设计的一种“级联端口”，一般都标有“UPLink”字样。因为有两种级联方式，所以事实上所有的集线器都能够进行级联，至少可以通过普通端口进行。

（1）使用 UpLink 端口级联。大多数集线器都会带有 UpLink 端口，当使用集线器提供的专门用于上行连接的 UpLink 端口时，通常可利用直通跳线的双绞线将该端口连接至其他集线器上除 UpLink 端口外的任意端口。

（2）使用普通端口级联。集线器间除了可以使用专用级联端口（UpLink 端口）进行级联外，还可以通过集线器的普通端口进行级联。要注意的是，这时的连接双绞线要用反线，也就是说双绞线的两端要跳线。反跳的方法是，一端的第 1～3 脚与第 2～6 脚下对调。

从以上两种集线器端口扩展连接方式（“堆叠”与“级联”）可以看出，堆叠方式实现起来比较困难，投资较大，而且集线器间的距离也受到很大限制。级联方式相对来说实现起来比较容易，投资也较便宜（带有级联端口的集线器很丰富，而且也不是很贵，并且还可以通过普通端口来实现级联），在距离上也有很大余地，可以达到单段双绞线网段的最大距离 100m，实现起来比较灵活。但是，堆叠方式在性能方面比级联方式更具有优势，而且堆叠方式可以实现多台集线器统一管理。

集线器间的级联除了能够增加集线器的端口数量外，另一个重要作用是延扩局域网络的范围（其实，同时也扩展了集线器的端口数）。对于 10Base-T 网络而言，非屏蔽双绞线所允许的最长传输距离为 100m，也就是说，网络范围是以集线器为中心的 100m 范围，这对于一

个较大型的网络来说肯定是远远不够的。当计算机与集线器的距离超过 100m 时，就可以通过在线路的中间加一个集线器的方法来实现距离的扩展，计算机到集线器以及集线器到集线器的距离均小于 100m 就可以解决上述问题。虽然集线器级联方式有 UpLink 端口方式和普通端口方式两种，但从网络连接距离来考虑，最好选用 UpLink 端口方式，因为这种连接方式可以最大限度地保证下一个集线器的带宽和信号强度；而采用普通端口进行扩展时，信号衰减严重，而且带宽受网络影响较大，这是多级级联的网络比较注重的问题。

2.5 交换机概述

交换机的品牌众多，在我国市面上的主流品牌有华为、3COM、Cisco、Accton、D-Link、TP-Link、联想等。

2.5.1 透明网桥

网桥是一种帧存储转发设备，用来连接两个相似类型的局域网。从协议的层次看，网桥是在数据链路层对数据帧进行存储转发。

1．网桥的功能

（1）过滤和转发。当网桥接收到数据帧时，先检查数据帧的源 MAC 地址和目的 MAC 地址，如果目的 MAC 地址和源 MAC 地址不在同一网络中，网桥就将该数据帧转发到另一个网络中；若目的 MAC 地址和源 MAC 地址在同一网络中，网桥就将该帧丢弃，起到对数据帧的过滤的作用。

（2）协议转换。在不同局域网之间进行互连时，由于各种局域网采用的介质访问控制方式不同，所以帧的格式也不一样。网桥的协议转换功能就是将源局域网的帧格式转换成目标局域网的帧格式。

（3）缓冲管理。在网桥中通常设置两类缓冲区：接收缓冲区和发送缓冲区。接收缓冲区用于暂存由源端口发来的帧，发送缓冲用于暂存已经经过帧格式转换并等待发往相邻局域网的帧。缓冲管理的功能就是保证缓冲区不溢出。

2．网桥的分类

根据路径选择方法，网桥分为透明网桥和源站选路网桥。

（1）透明网桥（Transparency Bridge）。“透明”是指局域网上的站点并不知道所发送的帧将经过哪几个网桥，网桥对各个站点来说是看不见的。这是以太网上用得最多的一种网桥。

（2）源站选路网桥（Source Routing Bridge）。由发送帧的源站点负责路由选择，源站选路网桥假定了每一个站在发送帧时都已经清楚知道发往各个目的站的路由，因而在发送帧时将详细的路由信息放在帧的首部中。

3．透明网桥的工作原理

透明网桥的工作原理如图 2.8 所示。

透明网桥有寻址和路径选择能力，路径选择采用查表法。网桥内的转发表描述了到达每个站点的路径，转发表主要由端口号和站点 MAC 地址组成。对于从端口收到的每个报文，查看其目的 MAC 地址，并与转发表对照，若目的 MAC 地址在接收端口的表项中，则丢弃报文（过滤）；若目的 MAC 地址在另一端口的表项中，则把报文转发到与该端口连接的网段（转发）；若目的 MAC 地址不在表中，则向接收端口外的其他所有端口广播该报文（广播）。

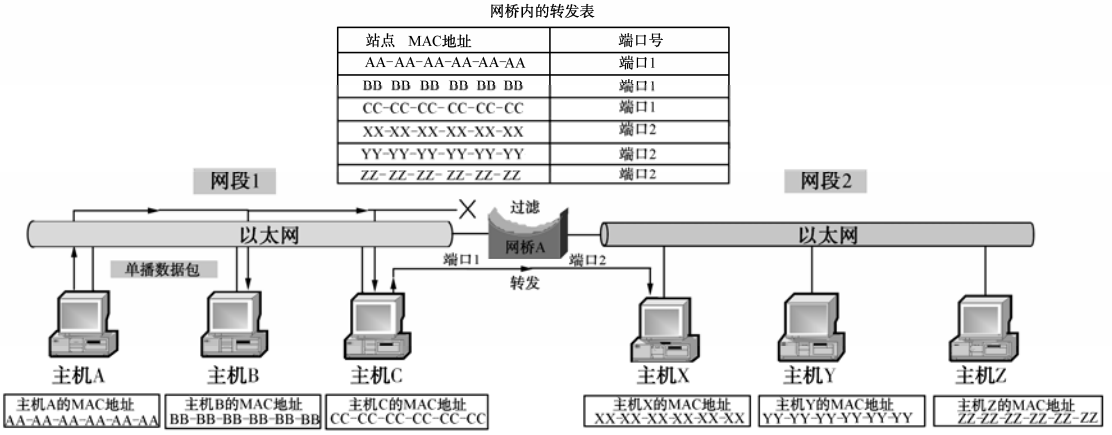


图 2.8　透明网桥的工作原理

2.5.2　交换机的交换方式

交换机通常具有多个端口，每个端口都直接与主机相连。可以把交换机看成是多端口的透明网桥。当主机需要通信时，交换机能同时连通许多对的端口，使每一对相互通信的主机都能像独占通信介质那样，进行无冲突的数据传输。

1．交换机的工作原理

交换机的工作原理与透明网桥的工作原理类似，也是存储转发。它将某个端口发送的数据帧先存储下来，通过解析数据帧，得到目的 MAC 地址，然后在交换机的 MAC 地址表（端口与 MAC 地址对应表）中，查找该目的主机所连接的交换机的端口，找到后就立即将数据帧转发到相应的端口。如果在地址表中找不到目的 MAC 地址对应的端口，则采用广播的方式，将数据帧广播到所有的端口，接收到回应后，交换机就知道目的主机所连接的端口，然后再将数据帧转发到相应的端口。之后，该 MAC 地址与端口的对应关系就记录在 MAC 地址表中，以后再发往该 MAC 地址的帧，就可以直接转发了。这就是交换机的地址学习功能。当有主机接入交换机后，交换机即开始学习该主机的 MAC 地址，并将学到的地址保存在 MAC 地址表中。

图 2.9 表示在 MAC 地址表还没有建立好之前，主机 D 向主机 C 发送数据帧的过程。交换机读取数据帧的源 MAC 地址，将主机 D 的 MAC 地址 0011.5B2C.DDDD 登记到 MAC 地址表中，对应交换机的 E3 端口。在交换机的地址表中找不到该数据帧的目的主机 C 的 MAC 地址 0011.5B2C.CCCC，就将该帧向交换机除 E3 以外的其他所有端口广播。

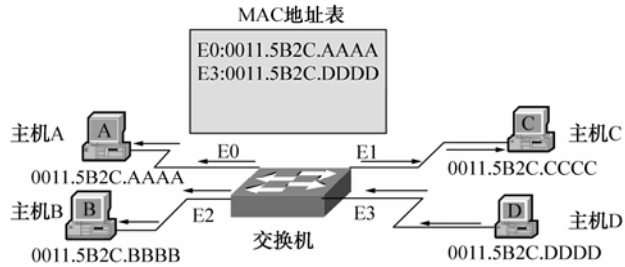


图 2.9　交换机进行地址学习、数据广播

图 2.10 表示在 MAC 地址表建立好后，主机 A 向主机 C 发送数据帧的过程。目的 MAC 地址（主机 C 的 MAC 地址）0011.5B2C.CCCC 可以在 MAC 地址表中查到，对应的端口为 E1，数据直接转发到 E1 端口，而不再向其他端口转发。

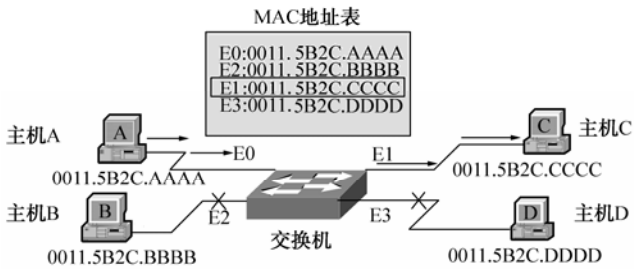


图 2.10　交换机进行数据转发

2．交换机的交换方式

交换机的交换方式有三种：存储转发方式、直通方式和无碎片直通方式。现在，大多厂商生产的以太网交换机都支持这三种交换方式，并且还可以根据网络数据转发的状况在这三种方式之间自动切换。

（1）存储转发方式（Store-And-Forward）。在存储转发方式下，交换机将整个帧复制到它的缓冲区里，然后计算 CRC（Cyclical Redundancy Check，循环冗余检验），如果 CRC 不正确，帧将被丢弃；如果正确，交换机查找目的 MAC 所在端口然后转发给它们。由于帧的长度可能不一样，所以转发延时根据帧的长短而变化。

（2）直通方式（Cut-Through）。使用直通方式时，交换机不必将整个的数据帧先缓存再进行处理，而是在接收帧的同时就立即按帧的目的 MAC 地址决定帧的转发端口，因而提高了帧的转发速度。直通方式的缺点是，它不检查 CRC 就直接将帧转发出去，因此也会将无效帧转发出去。

（3）无碎片直通方式（Fragment Free Cut-Through）。采用无碎片直通方式时，交换机接收到一帧的前 64 字节后，再进行转发操作，小于 64 字节的帧不转发。由于以太网中规定小于 64 字节的帧为无效帧，采用碎片直通转发时，降低了错误帧转发的概率。但是，对于长度大于 64 字节的错误帧仍会转发，转发延时大于直通方式。

三种交换方式需要处理的数据长度如图 2.11 所示。

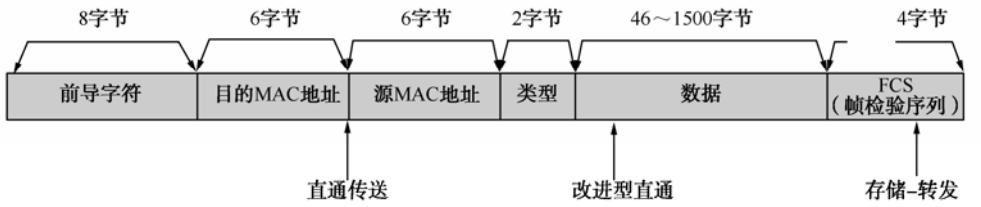


图 2.11　交换机的数据转发方式

3．网桥和交换机的比较

交换机可看成是多端口的网桥，两者均通过检查收到帧的源 MAC 地址来进行地址学习，两者均根据目的 MAC 地址来做转发决定，两者均转发二层广播。它们最大的区别在于网桥

基于软件，交换机基于硬件。

2.5.3 交换机的特性

1．每个端口独享带宽

交换机拥有一条高带宽的背板和内部交换矩阵，并为每个端口都设立了独立的通道和带宽，交换机的所有端口都挂接在这条背板总线上，通过内部的交换矩阵可以实现高速的数据转发。交换机通过内部的交换矩阵把网络划分为多个网段，每个端口为一个冲突域。与集线器的共享带宽不同，交换机的各个端口是独享带宽，可以实现全双工通信。交换机能够同时在多对端口间无冲突地交换帧。

2．增大了总带宽

若交换机的每个端口的带宽为 B_W，共有 n 个端口，则由该交换机构成的网络的总带宽等于（$B_W \cdot n$）/2 或 $B_W \cdot n$，其中（$B_W \cdot n$）/2 为所有端口以半双工通信方式工作时的总带宽，$B_W \cdot n$ 为全双工通信时的总带宽。例如 $n=8$，$B_W=10$Mbps，全双工通信时的网络总带宽最高可达 80Mbps，连接到交换机端口上的每台计算机的带宽为 10Mbps 。

3．分割冲突域

交换机上的每一个端口构成一个冲突域，一台直接与 10Mbps 以太网相连接的计算机，有自己的冲突域，并且能够达到 10Mbps 的带宽。例如，如果一台 16 端口的交换机，各个端口都与一个设备相连，就会产生 16 个冲突域。

采用交换机的网络虽然可以提高数据交换的处理能力、分割冲突域，但交换机对于广播的数据是要进行转发的，所以连接在交换机上的设备仍然处于同一个广播域。要隔离广播域，可以使用路由器来实现。由于路由器的成本较贵，比较经济的隔离广播域的方式是采用虚拟局域网（VLAN）。

2.5.4 交换机的分类

交换机的分类方式比较多，根据不同的分类标准，可以有多种的分类方法。下面介绍几种主要的分类方法。

1．按照覆盖范围分

（1）广域网交换机。主要是应用于电信级的城域网互连、互联网接入等领域的广域网中，提供通信应用的基础平台。

（2）局域网交换机。也就是我们平常所说的交换机，主要应用于局域网，用于连接终端设备，如服务器、客户机、集线器、路由器及打印机等网络设备，提供高速独占的网络通道。

2．按连接的网络类型分

（1）以太网交换机。以太网交换机是目前普遍使用的交换机。

（2）ATM 交换机。ATM 交换机用于电信、邮政网的主干网，其交换机产品在市场上很少看到。

3．按应用的层次分

（1）电信级交换机。主要用做电信级运营商的城域网骨干交换机。一般来说，能支持几千个信息点以上的交换机为电信级交换机，如图 2.12 所示。

图 2.12　电信级交换机

（2）企业级交换机。企业级交换机属于高端交换机，可为中、小企业骨干或大型企业配线间构建高速局域网。一般来说，能支持 500 个信息点以上的大型企业应用的交换机为企业级交换机，如图 2.13 所示。

图 2.13　企业级交换机

（3）部门级交换机。部门级交换机面向部门级网络，一般认为支持 300 个信息点以下的中、小企业的交换机为部门级交换机，如图 2.14 所示。

图 2.14　部门级交换机

（4）工作组级交换机。工作组级交换机是传统集线器的替代产品，一般认为支持 100 个信息点以下的交换机为工作组级交换机，如图 2.15 所示。

（5）桌面型交换机。桌面型交换机是一种低档交换机，如图 2.16 所示。支持的端口数较少，只具备最基本的交换机特性，价格也是最便宜的。

图 2.15　工作组级交换机

图 2.16　桌面型交换机

4．按照交换机的结构分

（1）固定端口交换机。固定端口交换机（如图 2.17 所示）所带的端口是固定的，不能进行扩展。

（2）模块化交换机。模块化交换机（如图 2.18 所示）提供更大的灵活性和可扩充性，用户可以任意选择不同数量、不同速率和不同接口类型的模块，以适应多变的网络需求。

图 2.17　固定端口交换机

图 2.18　模块化交换机

5．按照工作协议的层次分

（1）二层交换机。二层交换机根据数据链路层的 MAC 地址完成不同端口之间的数据转发，一般用于小型网络。

（2）三层交换机。三层交换机具有路由功能，能识别网络层的 IP 信息，将 IP 地址用于网络路径的选择。当网络规模较大时，不得不划分 VLAN 以减小广播域时，就必须使用三层交换机来实现 VLAN 间的线速路由。三层交换机一般用于大型网络。

（3）四层交换机。四层交换机工作在传输层，使用传输层包含在每一个 IP 包头中的服务或协议进行交换和传输处理、实现带宽分配、对数据流进行访问控制等。由于技术和价格方面的原因，目前实际应用还很少。

2.6　路由器的基础知识

2.6.1　路由器硬件介绍

路由器用于多个网络的互连，是智能的网络设备，主要工作在 OSI 参考模型的第三层。路由器的工作原理决定了数据包的传递机制。路由器的一个重要的功能就是检查流入的数据包，并要根据保存在路由表中的信息进行路由选择。路由器能通过第三层地址识别路由，这使得路由器能通过网络层寻址互连不同的多个网络，而无论它们之间的距离远近。

路由器可看成是专用的计算机，它与普通计算机一样也是由硬件和软件两部分构成。路由器的硬件主要由 CPU、存储器和一些接口组成，软件部分主要是指路由器的操作系统和一些配置文件。

1．CPU

路由器和 PC 一样，有中央处理单元 CPU，而且不同的路由器，其 CPU 一般也不相同。CPU 是路由器的处理中心，它负责执行处理数据包所需的工作。

2．存储器

存储器是路由器存储信息和数据的地方，路由器有以下几种存储组件。

（1）ROM（Read Only Memory，只读存储器）。ROM 中存储路由器加电自检（POST：Power-On Self-Test）、启动程序（Bootstrap）和部分或全部 IOS。ROM 是不可擦写的，ROM 中的软件升级需替换主板上的相应芯片。

（2）NVRAM（Nonvolatile Random Access Memory，非易失性 RAM）。NVRAM 中存储路由器的启动配置文件。重启或关闭路由器后，内容仍旧保持。

（3）闪存（Flash Memory）。闪存是一种可擦写的、也可编程的只读存储器（EPROM）。

闪存用于存储 IOS 软件和代码，维持路由器的正常工作。如果闪存的容量足够，则可在闪存中保存多个 IOS 映像文件，以提供多重启动选项。对路由器的 IOS 进行升级，就是指的对闪存中的 IOS 映像文件的版本进行升级。重启或关闭路由器后，内容仍旧保持。

（4）RAM（Random Access Memory，随机存取存储器）。RAM 与 PC 上的内存相似，提供临时信息的存储，在路由器通电后，同时保存着当前的路由表和配置信息。重启或关闭路由器后，RAM 中的内容丢失。

路由器软件与存储器的关系如表 2.1 所示。

表 2.1　路由器软件与存储器的关系

文件类型	名称	存放位置	运行位置
引导文件	Bootstrap	ROM	RAM
IOS 映像（Image）文件	Cisco IOS	Flash	RAM
配置文件	Running-Config	RAM	RAM
	Startup-Config	NVRAM	RAM

3．路由器接口

路由器上的三种基本类型接口为局域网接口、广域网接口和管理端口。

1）局域网接口

路由器能连接的局域网介质通常是某种类型以太网（以太网、快速以太网或千兆位以太网），也可以是其他技术的局域网，如令牌环或 FDDI。

2）广域网接口

广域网接口提供了通过某一服务提供商到达一个远端点或接入 Internet 的连接。由于路由器型号的不同，接口数目和类型也不尽一样。常见的接口主要有以下几种。

（1）高速同步串口，可连接 DDN、帧中继（Frame Relay）、X.25、PSTN（公共电话交换网）。

（2）同步/异步串口，可用软件将端口设置为同步工作方式。

（3）AUI 端口，即粗缆接口。需要外接转换器（AUI-RJ45），连接 10Base-T 以太网。

（4）ISDN 端口，可以连接 ISDN（2B+D），可作为局域网接入 Internet。

3）管理端口

管理端口的功能与其他各种接口不同。局域网和广域网接口提供的是分组传递所需的网络连接。管理端口提供一个基于文本的连接，用于完成路由器的配置和故障排除。常用的管理接口是 Console 端口（Console Port，控制台端口）和 AUX 端口（Auxiliary Port，辅助端口）。

（1）Console 端口，该端口为 EIA/TIA-232 的异步串行接口，主要连接终端或运行终端仿真程序的计算机，在本地配置路由器。

（2）AUX 端口，该端口与 Console 端口一样也是 EIA/TIA-232 的异步串行接口，主要用于远程配置备份，可与 MODEM 连接拨号，实现对路由器的远程配置和管理。

2.6.2　路由器工作原理

为了简单地说明路由器的工作原理，下面假设一个简单的网络。如图 2.19 所示，A、B、C、D 四个网络通过路由器连接在一起，下面介绍路由器是如何发挥其路由、数据转发作用的。

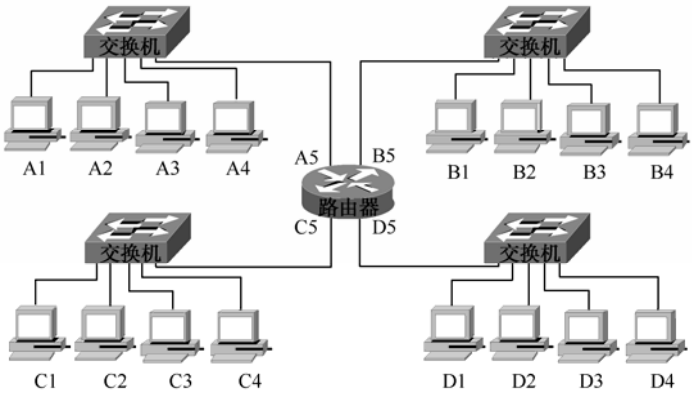


图 2.19　路由器的工作原理示意图

假设当网络 A 中的一个用户 A1 要向网络 C 中的用户 C3 发送一个请求信号时，信号传递的步骤如下：

（1）用户 A1 将目的用户 C3 的地址 C3，连同数据信息以数据帧的形式通过交换机用广播的形式发送给同一网络中的所有节点，当路由器 A5 端口侦听到这个地址后，分析得知所发目的节点不是本网段的，需要路由转发，就把数据帧接收下来。

（2）路由器 A5 端口接收到用户 A1 的数据帧后，先从报头中取出目的用户 C3 的 IP 地址，并根据路由表计算出发往用户 C3 的最佳路径。因为从分析得知 C3 的网络 ID 号与路由器的 C5 网络 ID 号相同，所以由路由器的 A5 端口直接发向路由器的 C5 端口应是信号传递的最佳途径。

（3）路由器的 C5 端口再次取出目的用户 C3 的 IP 地址，找出 C3 的 IP 地址中的主机 ID 号，如果在网络中有交换机，则可先发给交换机，由交换机根据 MAC 地址表找出具体的网络节点位置；如果没有交换机，则根据其 IP 地址中的主机 ID 直接把数据帧发送给用户 C3，这样就完成了一个完整的数据通信转发过程。

从上述内容可以看出，不管网络有多么复杂，路由器所做的工作就是这三步，所以整个路由器的工作原理基本上差不多。当然，在实际网络中远比图 2.19 所示的复杂得多，实际步骤也不会那么简单，但总的过程是这样的。

本 章 小 结

本章讲述了组成计算机企业网络的常用硬件的概念、分类、安装和选购等内容。

从大多数中、小型企业网的组建来看，主要用到各种通信线缆、网卡、集线器、服务器、交换机、路由器等硬件设备。本章从应用角度出发，重点讲述这些设备的概念、分类、安装和选购。

思 考 题

一、思考题

1．网卡的主要功能是什么？它一般由哪几部分组成？

2．如何在 Windows 系统中安装网卡驱动程序？

3．集线器的主要功能是什么？

4．集线器有哪些级联方式？各有什么用场？

5．试说明 5-4-3 准则。

二、填空题

1．网卡（Network Interface Card，NIC）也称_____，是计算机连接网络中各设备的接口。

2．网卡安装在网络计算机和服务器的扩展槽中，充当计算机和网络之间的_____接口。

3．网卡工作在物理层和_____之间。

4．_____是指网卡每秒接收可发送数据的能力，单位是 Mbps（兆位/秒）。

5．目前主流的网卡主要有 100Mbps 以太网卡、10Mbps/100Mbps 自适应网卡、以太网卡以及最新出现的万兆网卡等。

6．_____是目前服务器网卡经常使用的总线接口，它与原来的 PCI 相比在 I/O 速度方面提高了 1 倍。

7．_____ 接口网卡是最常见的一种网卡，也是应用最广的一种接口类型网卡，并且在双绞线以太网中应用普及。

8．一旦主连接因为数据线损坏或网络传输中断连接失败，备用连接会在几秒内自动顶替主连接的工作，通常网络用户不会觉察到任何变化，这主要通过_____技术实现。

9．网卡板材相当于电子产品的元器件材质，也是决定该产品的因素。较好的板材通常采用_____板。

10．_____是在网络环境中为客户机（Client）提供各种服务的、特殊的专用计算机。

11．WWW 服务器也称为_____或 HTTP 服务器，它是 Internet 上最常见也是使用最频繁的服务器之一。

12．_____是 Internet 的首要目的，即实现信息共享，文件传输是信息共享非常重要的内容之一。

13．_____用于把域名翻译成计算机能识别的 IP 地址。

14．_____给工作站提供各种服务，如网络通信服务、文件共享服务、硬件共享服务及各种资源服务。

15．_____ 是最低端服务器，其配置与普通的计算机差不多。

16．服务器硬盘是存储数据的仓库，所有的软件和_____都存储在这里。

17．网卡是计算机与_____相连的设备。

三、选择题

1．根据总线的类型不同，网卡可以分为_____。

A．ATM 网卡、令牌环网卡、以太网卡

B．10Mbps 网卡、100Mbps 网卡、10/100Mbps 网卡

C．工作站网卡、服务器网卡、笔记本网卡

D．ISA 网卡、PCI-X 网卡、PCI 网卡

2．MAC 地址通常存储在计算机的_____。

A．内存中

B．网卡中

C．硬盘中

D．高速缓冲区中

3．在以太网 10Base-TX 标准中，必须采用_____网卡。

A．10Mbps

B．100Mbps

C．10/100Mbps 自适应

D．100Mbps

4．按应用层次划分服务器时，可以分 4 种。下列选项中不正确的是_____。

A．基础级服务器

B．部门级服务器

C．工作组级服务器

D．企业级服务器

实训 1　网络通信线的连接与制作

一、实训目的

1．认识和熟练应用网线制作的专用工具。

2．进一步了解网络硬件的组成及各部分之间的关系。

3．掌握双绞线的制作方法。

二、实训环境

1．至少两台 PC。

2．每组配网线制作专用工具一套（剥线钳、细缆专用压钳、网钳等）。

3．每组以太网网卡两块，如 NE2000 型。

4．共用配集线器（Hub）一个、RJ-45 头两对、双绞线若干米。

5．配测线器一个。

三、实训内容

1．制作细缆网线一根（至少 0.5m）。

2．制作双绞线网线两根。

3．网络硬件的连接。

四、制作双绞线方法和步骤

1．制作工具和所需材料如下。

（1）专用工具一套：剥线工具、压线钳。

（2）3 类或 5 类 UTP 若干米。

（3）RJ-45 连接头若干。

2．制作步骤

3 类或 5 类 UTP 由 8 线 4 对呈螺线排列、两根导线相互扭绞在一起，并以坚韧的护套包裹着组成。其中 8 根导线以不同颜色区分，白橙与橙为一对，作为发送线对（TD＋、TD－）；白绿与绿为一对，作为接收线对（RD＋、RD－）；白蓝与蓝为一对，白棕与棕为一对，这两对没用，作为预留对。双绞线线色标准如表 2-2 所示。

表 2-2　双绞线线色标准

线色	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕
导线编号	1	2	3	4	5	6	7	8
信号	TD+	TD−	RD+	Not used	Not used	RD−	Not used	Not used

制作双绞线的具体步骤：

（1）剥出 1.5～2.0cm 的双绞线。左手持双绞线一端，右手持剥线工具，将双绞线夹在剥线工具刀口上。左手持线不动，右手将剥线工具旋转 3～4 圈，松开剥线工具，把剥开部分取下。

（2）分别将 4 对导线分开，并按导线编号 1、2、3、4、5、6、7、8 的顺序一字排列整齐，再用压线钳将其剪齐，留出 1cm 左右的双绞线头。

（3）将剪齐后的 8 根导线插入 RJ-45 连接头内。

（4）将插入 8 根导线后的 RJ-45 连接头放入双绞线专用压线钳的端口内，并用力压钳使得 RJ-45 头内刀片与 8 根导线牢牢相连。

（5）按上述同样的步骤压制双绞线的另一端（注意：导线的排列顺序应保持一致），一根双绞线即制作完成。

（6）使用万用表依次测试 RJ-45 连接头上的每一根线，或使用专用工具测试，必须保证全部接通。

五、实训报告要求

1．总结网络硬件的组成。

2．总结制作网线所需的工具及网络配件。

3．总结制作双绞线的方法与步骤。

4．画出网络硬件连接的示意图。

第 3 章　网络操作系统

本章要点

网络操作系统（Network Operation System，NOS）是网络的心脏和灵魂，它向网络计算机提供网络通信和网络资源共享功能，是负责管理整个网络资源和方便网络用户的软件的集合。

本章主要讲述网络操作系统的概念，网络操作系统的作用，介绍常见的几种网络操作系统 NetWare、Windows Server、UNIX/Linux 以及 Windows Server。

本章目标

- 理解网络操作系统的基本功能、资源共享和安全管理的基本原理及概念
- 理解网络操作系统的各种工作模式、文件系统格式和体系结构
- 了解市面上流行的几种网络操作系统
- 了解操作系统与网络操作系统的联系与区别
- 了解网络操作系统的最新技术和发展方向
- 掌握 Windows Server 的配置与使用方法

3.1　网络操作系统概述

操作系统随着人们对需求的不同有一个渐进的发展历程，从最早的单用户操作系统发展到多用户、多任务操作系统，又从单机操作系统发展到后来的网络操作系统。

网络操作系统是相对于单机操作系统而言的，指能使网络上每台计算机方便而有效地共享网络资源，为用户提供所需的各种服务的操作系统。

网络操作系统除了具备单机操作系统所需的功能（如内存管理、CPU 管理、输入/输出管理、文件管理等）外，还有网络通信、网络服务管理等网络功能。

操作系统是用户和计算机之间进行通信的接口，网络操作系统则是网络用户和计算机网络之间的接口。

3.1.1　网络操作系统的发展

1．早期的操作系统

最初的计算机没有操作系统，人们通过各种操作按钮来控制计算机。随后，为了提高效率而出现了汇编语言，操作人员通过有孔的纸带将程序输入计算机进行编译。这些将语言内置的计算机只能由操作人员自己编写程序来运行，不利于设备、程序的共用。为了解决这种问题，就出现了现代的操作系统。操作系统是人与计算机交互的界面，是各种应用程序共同的平台。有了操作系统，一方面很好地实现了程序的共用，另一方面也方便了对计算机硬件资源的管理。

1956 年，鲍勃 •帕特里克（Bob Patrick）在美国通用汽车的系统监督程序（System Monitor）的基础上，为美国通用汽车和北美航空公司在 IBM 704 机器上设计了基本的输入/输出系统，即 GM-NAA I/O。 GM-NAA I/O 可以成批地处理进程，在一项进程结束之后，它会自动地执行新的进程；它可以使用相关数据与命令来产生并执行新的命令与任务；它还为程序提供了统一的共享接口，使之可以访问计算机硬件的输入/输出接口。一般认为，这就是最早有记录的操作系统。其后，逐渐产生了 CP/M、C-DOS、M-DOS、TRS-DOS、S-DOS 和 MS-DOS 等操作系统。

早期的操作系统为单用户、单任务的操作系统。其中值得一提的是 MS-DOS，它是在 IBM-PC 及其兼容机上运行的操作系统，起源于 SCP86-DOS，是 1980 年基于 8086 微处理器而设计的单用户操作系统。后来，微软公司获得了该操作系统的专利权，配备在 IBM-PC 上，并命名为 PC-DOS。1981 年，微软公司的 MS-DOS 1.0 版与 IBM 的 PC 面世，这是第一个实际应用的 16 位操作系统。从此，微型计算机进入了一个新纪元。1987 年，微软公司发布的 MS-DOS 3.3 版本是非常成熟、可靠的 DOS 版本，微软公司据此取得个人操作系统的霸主地位。

从 1981 年问世至今，DOS 经历了 7 次大的版本升级，从 1.0 版到现在的 7.0 版，不断地改进和完善。但是，DOS 系统的单用户、单任务、字符界面和 16 位的大格局没有变化，因此，它对于内存的管理也局限在 640KB 的范围内。由此带来的很多局限性限制了 DOS 系统的进一步应用，Windows 系列操作系统是微软公司为了克服 DOS 系统的这些限制而开发出的。

2．现代操作系统

随着社会的发展，早期的单用户操作系统已经远远不能满足用户的要求，以多用户、多道作业和分时为特征的系统不断涌现出来，其典型代表有 UNIX、Windows、Linux 等操作系统。以推出的时间来说，UNIX 为最早，Netware 为第二，Windows NT 最晚。这些操作系统都有良好的用户界面，强大的网络功能，可靠的安全、稳定性能，支持多种硬件平台、多用户、多任务，支持多种文件系统等共同的特点。

在所有这些操作系统中，从微软公司于 1985 年推出 Windows 1.0 以来，Windows 系统从最初运行在 DOS 下的 Windows 3.x，到风靡全球的 Windows 9x/Me/2000/NT/XP/Vista，Windows 几乎成了操作系统的代名词。因此，说到操作系统的发展，无疑要多关注 Windows 系统。

Windows 是微软公司在 1985 年 11 月发布的第一代窗口式多任务系统，它使 PC 开始进入了图形用户界面时代。Windows 1.x 版是一个具有多窗口及多任务功能的版本，但由于当时的硬件平台为 PC/XT，速度很慢，所以 Windows 1.x 版本并未十分流行。1987 年年底，微软公司又推出了 MS-Windows 2.x 版，它具有窗口重叠功能，窗口大小也可以调整，并可把扩展内存和扩充内存作为磁盘高速缓存，从而提高了整台计算机的性能，此外，它还提供众多的应用程序。

1990 年，微软公司推出 Windows 3.0，它的功能进一步加强，具有强大的内存管理，并且提供数量相当多的 Windows 应用软件，因此成为 386、486 微机新的操作系统标准。随后，微软公司推出了 Windows 3.1 版，而且推出了相应的中文版。3.1 版与 3.0 版相比，增加了一些新的功能，受到了用户欢迎，是当时最流行的 Windows 版本。

1995 年，微软公司推出了 Windows 95。在此之前的 Windows 都是由 DOS 引导的，也就是说它们还不是一个完全独立的系统，而 Windows 95 是一个完全独立的系统，并在很多方面

做了进一步的改进，还集成了网络功能和即插即用功能，是一个全新的 32 位操作系统。1998 年，微软公司推出了 Windows 95 的改进版 Windows 98，Windows 98 的最大的特点是，把微软公司的 Internet 浏览器技术整合到 Windows 95 中，使得访问 Internet 资源就像访问本地硬盘一样方便，从而更好地满足了人们越来越多的访问 Internet 资源的需要。Windows 2000 于 2000 年 2 月 17 日正式推出，针对不同的用户群体共发布了 4 个版本：Professional（专业版）、Server （服务器版）、Advanced Server （高级服务器版）以及 Datacenter Server （数据中心服务器版），标志着微软公司开始向服务器市场发起了强有力的冲击。

Windows Server 2003 于 2003 年 3 月 28 日问世。针对不同的商业需求，Windows Server 2003 进一步细分了版本子集，包括 Web 版、标准版、企业版和数据中心版这 4 个版本。在对 Windows 2000 中的活动目录、组策略操作和管理、磁盘管理等众多服务器组件做了较大改进后，Windows Server 2003 在稳定性和安全性上有了实质性的飞跃。

3．未来操作系统的发展趋势

未来的操作系统应易于满足用户的各种需求。最受用户关注的三个因素是安全性、易操作性、界面友好。体现为以下的三种功能特点：

（1）比以往更加强大的集成搜索功能。以往的操作系统仅仅支持按文件类型、文本文件进行全文搜索，而新的操作系统做了很大改进，如支持电子数据表、演示片、电子邮件信息、最近访问过的网站内容、图像或图片标签、短信聊天和即时聊天内容、PDF 文件内容搜索，等等。同样，新的操作系统除具有很强的搜索功能外，还有其他特色功能，如输入用户想执行的工作，相应的应用程序会自动打开。

（2）更加绚丽的桌面和 3D 视觉效果。在桌面显示视觉效果和 3D 加速图形能力方面，比以往有很大提升，并且各有特点，如在 Vista 中采用了半透明的窗口，图片显示效果更加绚丽，显示的图标立体感更强。

（3）系统安全度有很大提升。随着用户使用水平的不断提高，用户对网络操作系统的安全性要求也越来越高。例如，在 Vista 操作系统中，设定了新的用户账户等级程序、高级数据保护技术，降低了数据被未授权用户查看的风险，支持硬件全卷加密以防止其他操作系统从磁盘访问文件，具有全新的防火墙程序，使用安全性更强的 IE7 等多重手段来提高其安全性。

3.1.2 网络操作系统的分类

网络操作系统可分为对等结构和非对等结构的网络操作系统。

1．对等结构网络操作系统

对于小型局域网，主要的应用是在小组内共享数据和打印机等资源，不需要专门的中央处理器。局域网上为数不多的 PC 需要相互通信和共享一些资源。在每个 PC 上安装相同类型的操作系统，连网计算机的资源在原则上都是可以相互共享的。专门为这种结构开发的网络操作系统称为对等结构网络操作系统，它们的价格比较低廉。比较流行的有两种：Novell 公司推出的 NetWare Lite（后又改为 Personal Netware）和微软公司推出的 Windows for Workgroups。图 3.1 是典型的对等结构局域网的结构图。

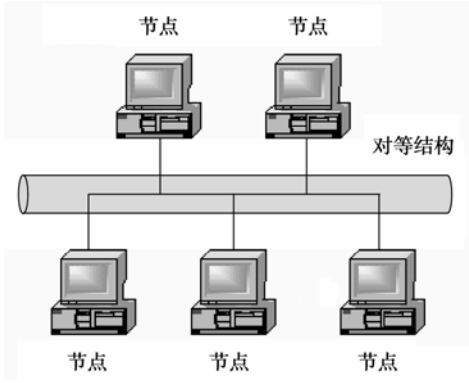


图 3.1　典型的对等结构局域网的结构图

2．非对等结构网络操作系统

在非对等结构的局域网中，连网节点分为网络服务器（Network Server）和网络工作站（Network Workstation）两类。图 3.2 是典型的非对等结构局域网的结构图。

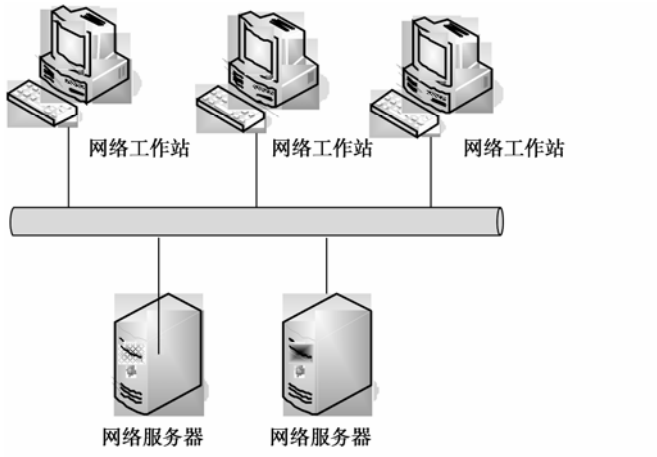


图 3.2　非对等结构局域网的结构图

网络服务器采用高配置与高性能的计算机，以集中方式管理局域网的共享资源，并为网络工作站提供各类服务。网络工作站一般是配置比较低的微型机系统，主要为本地用户访问本地资源与访问网络资源提供服务。

现代的大多数网络操作系统都采用非对等结构。常见的有 NetWare 系列、Windows 系列以及 UNIX 操作系统。

3.1.3　网络操作系统的服务功能

网络操作系统作为网络用户和计算机之间的接口，通常具有复杂性、并行性、高效性和安全性等特点。因此，网络操作系统除了应具有普通操作系统具有的处理机管理、存储器管理、设备管理和文件管理等基本功能外，一般要求网络操作系统还具有如下功能。

（1）支持多任务：要求操作系统在同一时间能够处理多个应用程序，每个应用程序在不同的内存空间运行。

（2）支持大内存：要求操作系统支持较大的物理内存，以便应用程序能够更好地运行。

（3）支持对称多处理：要求操作系统支持多个 CPU 减少事务处理时间，提高操作系统性能。

（4）支持网络负载平衡：要求操作系统能够与其他计算机构成一个虚拟系统，满足多用户访问时的需要。

（5）支持远程管理：要求操作系统能够支持用户通过 Internet 远程管理和维护，如 Windows Server 2003 操作系统支持的终端服务。

3.2 局域网中常用的网络操作系统

局域网中的网络操作系统有两个基本的要求：一是允许在局域网上的共享资源，二是使现有的 PC 操作系统仍能继续运行，而不需要做任何改变。为了满足这两个基本要求，网络操作系统有两个组成：一是控制服务器的操作管理存储在服务器上的文件，二是运行在客户系统的软件，使客户能访问网络及网上资源。局域网中常用的网络操作系统有 NetWare、Windows、UNIX、Linux 等。

3.2.1 NetWare操作系统简介

NetWare 操作系统虽然远不如早几年那么风光，在局域网中早已失去了当年雄霸一方的气势，但是 NetWare 操作系统仍以对网络硬件的要求较低（工作站只要是 286 机就可以）而受到一些设备比较落后的中、小型企业的青睐。人们一时还忘不了它在无盘工作站组建方面的优势，还忘不了它那毫无过分需求的大度。并且，它兼容 DOS 命令，其应用环境与 DOS 相似，经过长时间的发展，具有相当丰富的应用软件支持，技术完善、可靠。目前常用的版本有 V3.11、V3.12 和 V4.10、V4.11、V5.0 等中/英文版本，NetWare 服务器对无盘站和游戏的支持较好，常用于游戏厅。目前，这种操作系统的市场占有率呈下降趋势，这部分的市场主要被 Windows NT/2000 和 Linux 系统瓜分了。

3.2.2 Windows操作系统

Windows 操作系统是全球最大的软件开发商——微软（Microsoft）公司开发的。微软公司的 Windows 操作系统不仅在个人操作系统中占有绝对优势，它在网络操作系统中也非常强劲。这类操作系统配置在整个局域网中是最常见的，但由于它对服务器的硬件要求较高，并且稳定性能不是很高，所以微软的网络操作系统一般只用在中、低档服务器中，高端服务器通常采用 UNIX、Linux 或 Solaris 等非 Windows 操作系统。在局域网中，微软的网络操作系统主要有 Windows NT 4.0 Server、Windows 2000 Server/Advance Server 以及 Windows Server 2003/2008 等，工作站系统可以采用任一种 Windows 或非 Windows 操作系统，包括个人操作系统，如 Windows 9x/ME/XP 等。

在整个 Windows 网络操作系统中，最为成功的是 Windows NT 4.0 Server 系统，它几乎成为中、小型企业局域网的标准操作系统：一是它继承了 Windows 家族的统一界面，使用户学习、使用起来更加容易；二是它的功能比较强大，基本上能满足所有中、小型企业的各项网络需求。虽然与 Windows 2000/2003 Server 系统相比，Windows NT 4.0 Server 系统在功能上逊色许多，但它对服务器的硬件配置的要求低许多，可以更大程度地满足许多中、小企业的 PC 服务器配置需求。

3.2.3 UNIX/Linux操作系统简介

目前常用的 UNIX 操作系统的版本主要有 UNIX SUR 4.0、HP-UX 11.0，SUN 的 Solaris 8.0 等，支持网络文件系统服务，提供数据等应用，功能强大，由 AT&T 和 SCO 公司推出。UNIX 网络操作系统的稳定和安全性能非常好，但由于它多数是以命令方式来进行操作的，不容易掌握，特别是初级用户。正因如此，小型局域网基本不使用 UNIX 作为网络操作系统，UNIX 一般用于大型的网站或大型的企、事业局域网中。UNIX 网络操作系统的历史悠久，其良好的网络管理功能已为广大网络用户所接受，拥有丰富的应用软件的支持。目前，UNIX 网络操作系统的版本有 AT&T 和 SCO 公司的 UNIX SVR 3.2、SVR 4.0 和 SVR 4.2 等。UNIX 本是针对小型机主机环境开发的操作系统，是一种集中式分时多用户体系结构。因其体系结构不够合理，UNIX 的市场占有率呈下降趋势。

Linux 是一种新型网络操作系统，它的最大的特点是源代码开放，可以免费得到许多应用程序。目前也有中文版本的 Linux，如 Red Hat（红帽子）、红旗 Linux 等。Linux 在国内得到了用户充分的肯定，主要体现在它的安全性和稳定性方面，它与 UNIX 有许多类似之处。目前，这类操作系统主要应用于中、高档服务器中。

总的来说，对特定计算环境的支持使得每一个操作系统都有适合于自己的工作场合，这就是系统对特定计算环境的支持。例如，Windows 2000 Professional 适用于桌面计算机，Linux 适用于小型网络，Windows 2000 Server 和 UNIX 适用于大型服务器应用程序。因此，对于不同的网络应用，需要我们有目的地选择合适的网络操作系统。

3.3 Windows网络的基本概念

Windows 网络操作系统通常采用以下三种方式来管理网络资源：

（1）工作组模式。

（2）客户机/服务器（C/S）模式。

（3）域模式。

3.3.1 Windows组网方式

1．工作组模式

如果网络规模较小，可以使用 Windows 工作组模式来进行管理，但其管理功能极其有限。“工作组”是比较基本的分组，只用于帮助用户查找组内打印机和共享文件夹之类的对象。“工作组”本身的作用是方便网上计算机共享资源的浏览。

工作组的特点是实现每台计算机的管理，适用于距离很近的有限数目的计算机。在每个工作组中，自动推选出一个主浏览器，负责维护本工作组所有计算机的 NetBIOS 名称列表。用户可以使用默认的工作组名 workgroup，也可以任意起个名字（不必担心重名），同一工作组或不同工作组间在访问时也没有限制，因为要访问目标计算机都需要输入目标计算机上的用户名、口令进行验证。

在工作组中，用户可能需要记住多个密码，因为每个网络资源都有自己的密码。（此外，不同的用户对每个资源可以使用不同的密码）。工作组的这种分散管理性是与域的集中式管理相比的最大缺点。

2．客户机/服务器（C/S）模式

在 C/S 模式中，资源集中存放在一台或者几台服务器上。如果只有一台服务器，则只需在服务器上为每个用户建立一个账户，用户只需登录该服务器就可以使用服务器中的资源。如果资源分布在多台服务器（如图 3.3 所示），则要在每台服务器分别为每个用户建立一个账户（共 $M \times N$ 个），用户需要在每台服务器上（共 M 台）登录，感觉又回到了工作组模式。

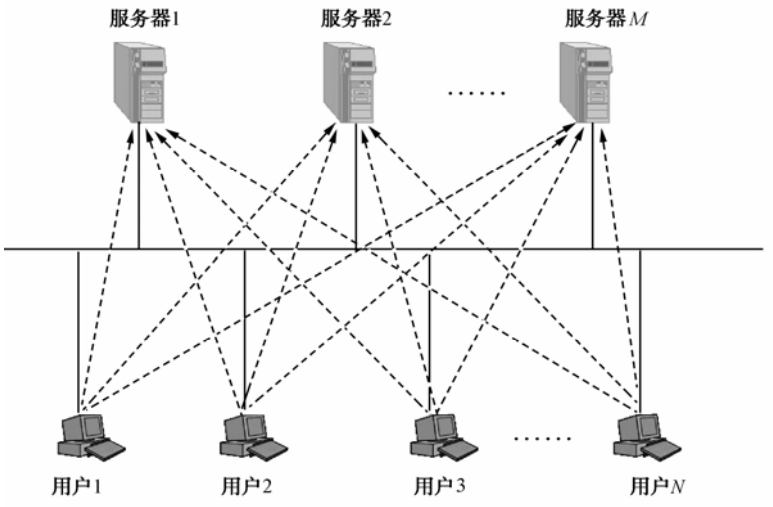


图 3.3　资源分布在多台服务器上

3．域模式

域提供了对网络资源的集中控制，用户只需登录一次就可以访问整个活动目录的资源。域是一组账户和网络资源，这些资源共享共同的目录数据库和安全策略集，并可能与其他域有安全关系，如图 3.4 所示。除了有几个用户的小型网络外，建议所有网络都使用域模式。

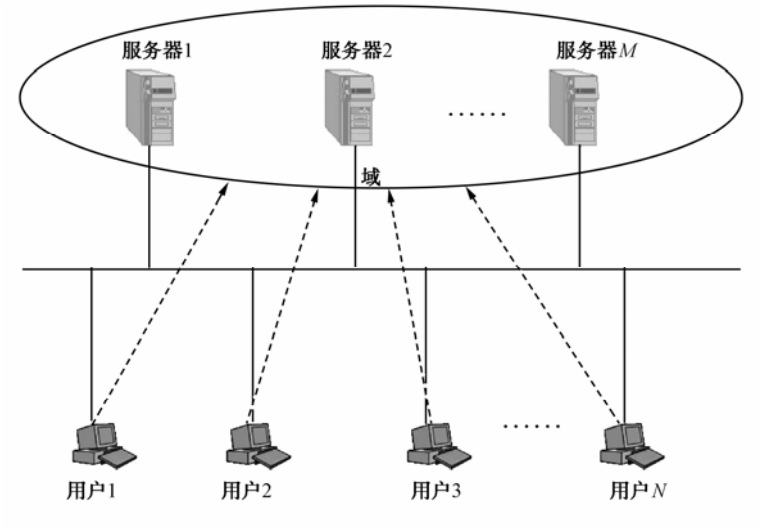


图 3.4　域的模式

在域中，比较容易跟踪密码和权限，因为域具有用户账户、权限和其他网络详细信息的

单个集中数据库。该数据库中的信息将自动在域控制器之间进行复制。要确定哪些服务器是域控制器，哪些服务器只是域成员。既可在安装过程中也可在安装完成后确定这些角色。

域及其所在的活动目录系统在维护极佳的监视和安全性的同时，还提供许多使资源易于被用户访问的选项。

3.3.2 活动目录

1．活动目录的基本概念

要想理解什么是活动目录（Active Directory），必须先了解什么是目录（Directory）和目录服务（Directory Service）。在计算机服务中使用的“目录”和现实生活使用的“目录”很相似，都是存储以某种方式相关联的对象的信息集，如同图书馆的书目索引区分区存储了不同类型图书的索引，读者根据这些索引就可以很容易地找到想要的图书。

目录服务是用户通过其提供的服务来使用目录中的信息，一般用于识别网络上的资源，并使用户和应用程序能访问这些资源，将这些资源集中存储、使用和管理这些资源的全部信息，因此，简化了查找和管理这些资源的过程。例如共享网络资源，没有目录服务时只能共享给所有人；有了目录服务就可以有针对性地将资源共享给某些需要的用户。在网络上查找打印机时候还可以很快地搜索到打印机。即使用户不知道资源的物理连接位置，也能够访问资源。

活动目录是一个分布式的目录服务。信息可以分散在多台不同的计算机上，保证快速访问和容错；无论用户从何处访问或这些资源处于何处，它都能对用户提供统一的视图。通过活动目录服务，管理员可以实现整个网络的集中管理。

2．活动目录的优点与特性

（1）与 DNS 集成。活动目录使用域名系统（DNS）。DNS 是一种 Internet 标准服务，它将用户能够读取的计算机名称（如 www.cec.edu.cn）翻译成计算机能够读取的数字 Internet 协议（IP）地址。这样，在 TCP/IP 网络计算机上运行的进程即可相互识别并进行连接。

（2）采用对象的管理。活动目录可对网络上的资源全部以对象进行管理。管理员在任何一台计算机上登录，就能管理网上任何一台机器上的对象。总的来说，分为对象类和对象属性，以便于对资源的管理和控制。创建对象时，属性就存储了描述该对象的信息。例如，用户类包含许多属性，如用户名属性、描述属性、电话号码属性等。

（3）增强的安全性。活动目录不仅可在目录中的每个对象上定义访问控制权限，而且还可在每个对象的属性上定义访问控制权限。

3．活动目录的结构

活动目录的结构主要指网络中所有用户、计算机以及其他网络资源的层次关系。通常情况下，活动目录的结构可以分为逻辑结构和物理结构。

活动目录的逻辑结构包括域、域树、域林和组织单元。

组织单元（Organizational Unit，OU）是一个容器对象，可以把域中的对象组织成逻辑组，以简化管理工作。组织单元可以包含各种对象，如用户账户、用户组、计算机、打印机等，甚至可以包括其他组织单元，可以利用组织单元把域中的对象组成一个完全逻辑上的层次结构。对于企业来讲，可以按部门把所有的用户和设备组成一个组织单元层次结构，也可以按地理位置形成层次结构，还可以按功能和权限分成多个组织层次结构。

活动目录的物理结构与逻辑结构有很大不同，它们是彼此独立的两个概念。逻辑结构侧重于网络资源的管理，而物理结构则侧重于网络的配置和优化。活动目录的物理结构，主要着眼于活

动目录信息的复制和用户登录网络时的性能优化。物理结构的两个重要概念是站点和域控制器。

站点由一个或多个 IP 子网组成，这些子网通过高速网络设备连接在一起。站点往往由企业的物理位置分布情况决定，可以依据站点结构配置活动目录的访问和复制拓扑关系，从而可使网络更有效地连接，并且可使复制策略更合理，用户登录更快速。活动目录中的站点与域是两个完全独立的概念，一个站点中可以有多个域，多个站点也可以位于同一域中。

域控制器指运行 Windows Server 的服务器，它保存了活动目录信息的副本。域控制器管理目录信息的变化，并把这些变化复制到同一个域中的其他域控制器（备份域控制器）上，使各域控制器上的目录信息同步。域控制器也负责用户的登录过程以及其他与域有关的操作，如身份鉴定、目录信息查找等。

活动目录支持多主机复制方案，然而由于复制引起的通信流量以及网络潜在的冲突，变化的传播并不一定能够顺利进行，因此有必要在域控制器中指定全局目录服务器以及操作主机。

全局目录是一个信息仓库，包含活动目录中所有对象的一部分属性，往往是在查询过程中访问最为频繁的属性。利用这些信息，可以定位到任何一个对象的实际所在位置。

有了域林之后，同一域林中的域控制器共享一个活动目录，这个活动目录是分散存放在各个域的域控制器上的，每个域中的域控制器存有该域的对象的信息。如果一个域的用户要访问另一个域中的资源，则这个用户必须能够查找到另一个域中的资源。为了让每一用户能够快速查找到另一个域内的对象，微软公司设计了全局编录（Global Catalog，GC）。

全局编录包含了整个活动目录中每一个对象的最重要属性（即部分属性，而不是全部），这使得用户或者应用程序即使不知道对象位于哪个域内，也可以迅速找到被访问的对象。

3.3.3 域的基本概念、组成

1．域

“域”是活动目录的一种实现形式，也是活动目录的最核心的管理单位和复制单位。在 Windows NT 中，引入了“域”的概念，将“域”作为一个基本的网络管理单位，它的作用是将网络中的用户账号数据库和安全性策略数据库进行统一管理。一个 Windows NT 网可以由多个域组成，这些域之间通过信任关系建立关联。

域是一个逻辑上的概念，与网络中计算机的物理连接方式是无关的，一个域由一台或多台服务器以及客户机组成。根据职责的不同，域中的服务器分为以下三类：

（1）基本域控制器（Primary Domain Controller），用来创建和维护共享资源、用户账号、安全性策略数据库，同时对用户的上网登录做出鉴别。

（2）备份域控制器（Backup Domain Controller），用来对基本域控制器的安全性信息做实时备份，另外它也可对用户的上网登录做出鉴别。这是 Windows NT 中使用双机备份这种系统容错技术的基本策略。

（3）域服务器（Domain Server），它为网络中的客户机提供某种专门的服务（如数据库服务、异步通信服务等），而不做大量的管理任务，也不鉴别用户的登录请求。

在一个域中必须有一个基本域控制器，而备份域控制器和域服务器是可选的。

2．多域模式与信任

在一个复杂的多域模型的网中，可以通过建立信任关系实施更进一步的集中管理。如果每个域都是彼此相互独立的，那么在整个网络环境中，就需要维护多个独立的数据库和管理方案。

所谓信任关系，就是指允许一个域的用户访问另一个域的资源。例如，如果域 A 信任域

B，那么域 B 上的用户可以登录到域 A 中，不管他在域 A 中有无账号。域之间的信任关系可以是单向的，也可以是双向的。但是，如果要实现 n 个域中的用户可以跨域访问资源，必须创建 $n\times(n-1)/2$ 个双向信任关系，如图 3.5 所示。

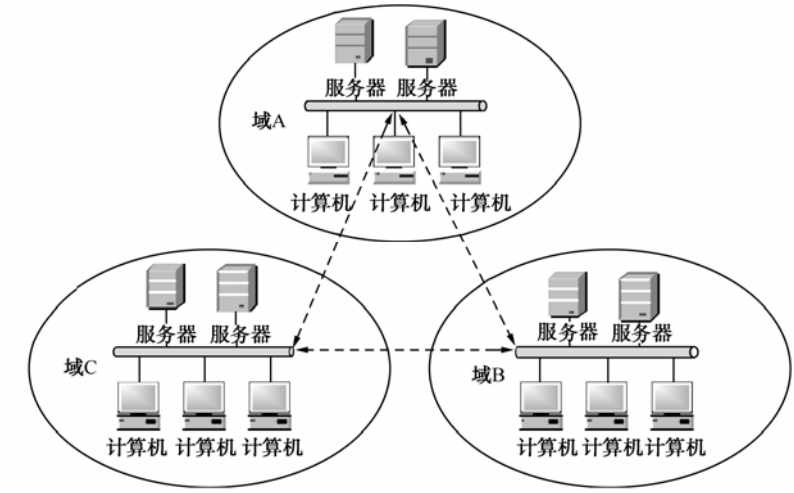


图 3.5　多域模式的信任关系

3．域树

从 Windows Server 2003 起，域树（Domain Tree）开始出现，域树中的域以树的形式出现。在域树中，父域和子域的信任关系是双向可传递的，因此域树中的一个域隐含地信任域树中所有的域，这种信任方式要建立的信任关系远比多域的方式少得多。对于如图 3.6 所示的 7 个域，只需要 6（$n-1$）个信任关系。

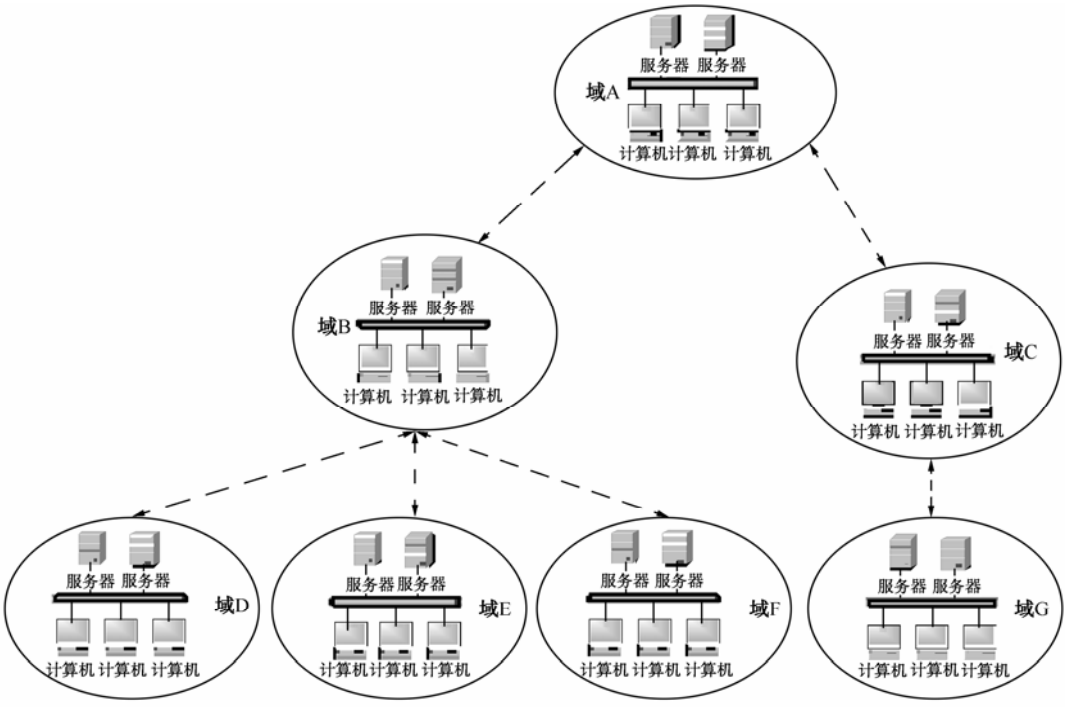


图 3.6　域树的信任关系

4．域林

域和 DNS 域的关系非常密切，因为域中的计算机使用 DNS 来定位域控制器、服务器以及其他计算机、网络服务等，实际上，域的名字就是 DNS 域的名字。在图 3.7 中，如果某学校已经有了一个域名 cec.edu.cn，现在因对外交流需要，学校又向 Internet 组织申请了一个新的 DNS 域名 cec.net。这时，学校可能同时拥有 cec.edu.cn 和 cec.net 两个域名，新域用 cec.net 作为域名，但是 cec.net 无法挂在 cec.edu.cn 域树中，这时只能单独创建另一个域树，如图 3.7 所示，新的域树根域为 cec.net，这两个域树共同构成了域林（Domain Forest）。

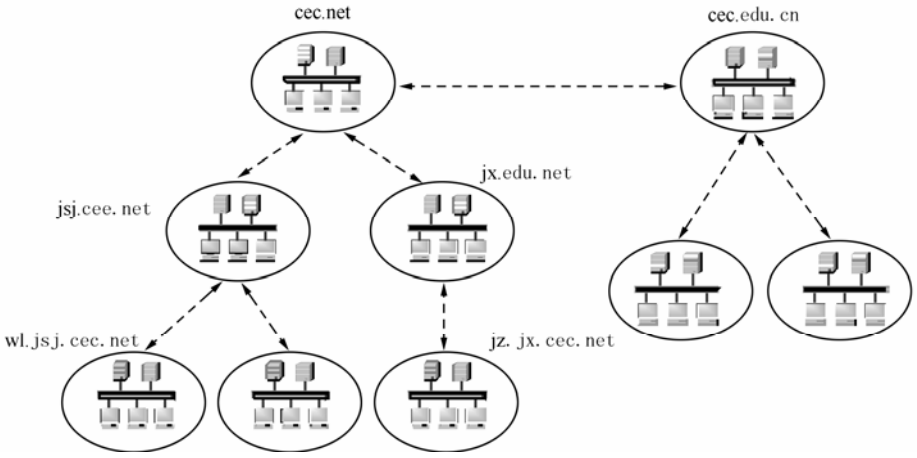


图 3.7　域林的信任关系

3.3.4　域控制器

在域模式下，至少有一台基本域控制器专门负责每一台连入网络的计算机和用户的验证工作。这个域控制器中包含由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当计算机连入网络时，域控制器首先鉴别这台计算机是否属于这个域，用户使用的登录账号是否存在，密码是否正确。如果以上信息之一不正确，那么域控制器就会拒绝这个用户从这台计算机登录。不能登录，用户就不能访问服务器上有权限保护的资源，他只能以对等网用户的方式访问 Windows 共享出来的资源，这样就在一定程度上保护了网络上的资源。

要把一台计算机加入域，仅仅使它和服务器在网上邻居中能够相互“查看”是远远不够的，还必须由网络管理员进行相应的设置，把这台计算机加入到域中。这样才能实现文件的共享。

1．服务器端设置

以系统管理员身份在已经设置好 Active Directory（活动目录）的 Windows Server 上登录，选择“开始”菜单的“程序”选项中的“管理工具”，再选择“Active Directory 用户和计算机”；在程序界面中右击“Computers”；在弹出的菜单中单击“新建”，然后选择“计算机”；填入想要加入域的计算机名，如图 3.8 所示。

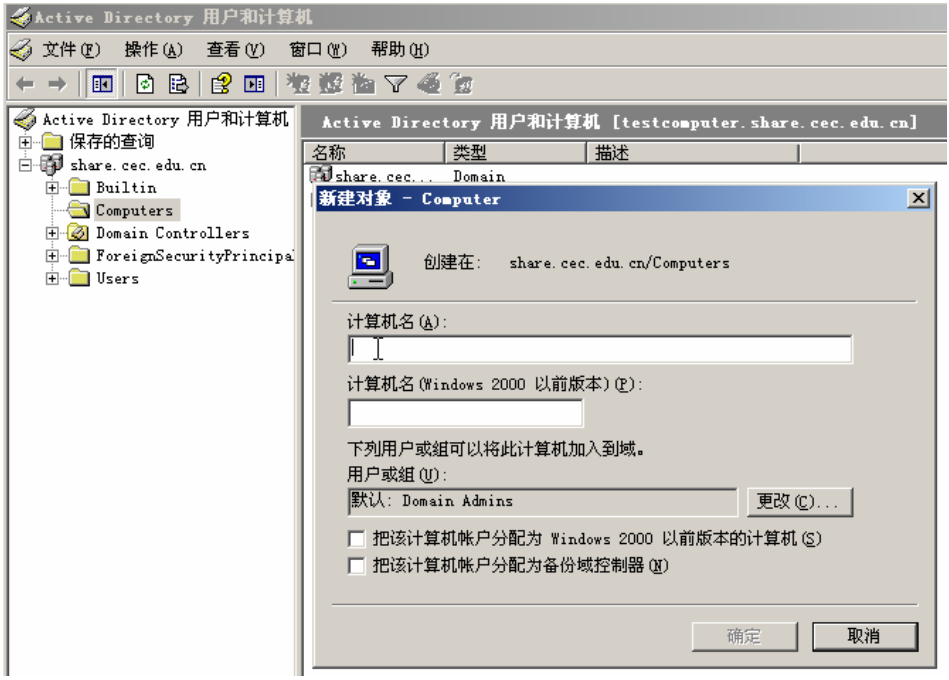


图 3.8　域控制器设置

2．客户端设置

首先确认计算机名称是否正确，然后在桌面的“网上邻居”上右击鼠标，单击“属性”出现网络属性设置窗口，确认“主网络登录”为“Microsoft 网络用户”。选中窗口上方的“Microsoft 网络用户”（如果没有此项，说明没有安装，单击“添加”安装“Microsoft 网络用户”选项）。单击“属性”按钮，出现“Microsoft 网络用户属性”对话框，选中“登录到 Windows NT 域”复选框，在“Windows NT 域”中输入要登录的域名。这时，如果是 Windows 98 操作系统，系统会提示需要重新启动计算机。重新启动计算机之后，会出现一个“登录”对话框。在输入正确的域用户账号、密码以及登录域之后，就可以使用 Windows Server 域中的资源。请注意，这里的域用户账号和密码，必须是网络管理员为用户建的那个账号和密码，而不是由本机用户自己创建的账号和密码。如果没有将计算机加入到域中，或者登录的域名、用户名、密码中有一项不正确，都会出现错误信息。

3.3.5　文件系统

文件系统是计算机用于组织硬盘上的数据的基本结构。如果要安装新硬盘，则需要使用文件系统对其进行分区和格式化，然后才能开始存储数据或程序。在 Windows 中，可以从中进行选择的三个文件系统选项为：NTFS、FAT32 以及现在很少使用的较早的 FAT（也称为 FAT16）。

NTFS 是此 Windows 版本的首选文件系统。与早期的 FAT32 文件系统相比，它有许多优点，其中包括：

（1）能够从某些与磁盘相关的错误中自动恢复，而 FAT32 则不能。

（2）改善了对较大硬盘的支持。

（3）由于可以使用权限和加密来限制许可用户访问特定文件，因此安全性更好。

NTFS 是 Windows NT 以及之后的 Windows 2000、Windows XP、Windows Server 2003、Windows Server 2008、Windows Vista 和 Windows 7 的标准文件系统。

NTFS 取代了文件分配表（FAT）文件系统，为 Microsoft 的 Windows 系列操作系统提供文件系统。NTFS 对 FAT 和 HPFS（高性能文件系统）做了若干改进，如支持元数据，并且使用了高级数据结构，以便于改善性能、可靠性和磁盘空间利用率；还提供了若干附加扩展功能，如访问控制列表（ACL）和文件系统日志。

FAT32 以及更少使用的 FAT 用于早期版本的 Windows 操作系统，包括 Windows 95、Windows 98 和 Windows Millennium Edition。FAT32 不具有 NTFS 提供的安全性，因此如果某计算机上有 FAT32 分区或卷，则访问该计算机的任何用户都可以读取其中的文件。FAT32 还有大小限制。不能在此 Windows 版本中创建大于 32GB 的 FAT32 分区，也不能在 FAT32 分区中存储大于 4GB 的文件。

使用 FAT32 的主要原因是，计算机有时需要运行 Windows 95、Windows 98 或 Windows Millennium Edition，有时又需要运行此 Windows 版本，这称为多重引导配置。如果是这种情况，则需要在 FAT32 或 FAT 分区中安装早期版本的操作系统并确保它是主分区（可以驻留操作系统的分区）。使用这些早期的 Windows 版本时，需要访问的其他任何分区也必须使用 FAT32 格式化。这些早期的 Windows 版本可以访问网络上的 NTFS 分区或卷，但不能访问计算机上的 NTFS 分区或卷。

Windows 2000 以上的操作系统提供了分区格式转换工具“Convert.exe”。Convert.exe 是 Windows 2000 以上的操作系统附带的一个 DOS 命令行程序，通过这个工具可以直接在不破坏 FAT 文件系统的前提下，将 FAT 转换为 NTFS。它的用法很简单，先在 Windows 2000 环境下切换到 DOS 命令行窗口，在提示符下键入：

C:\>convert 需要转换的盘符 /FS:NTFS

例如，E 盘原来为 FAT16/32，现在需要转换为 NTFS，可使用如下格式：

C:\>convert e: /FS:NTFS。

如果要转换操作系统所在分区（系统盘），所有的转换将在系统重新启动后完成。

此外，还可以使用专门的转换工具，如著名的硬盘无损分区工具 PowerQuest Partition Magic 7.0 软件，在此不再赘述。

本 章 小 结

本章主要介绍了网络操作系统的基本概念、网络操作系统的发展及常见的网络操作系统。

（1）网络操作系统可分为对等结构和非对等结构的网络操作系统。

（2）网络操作系统必须具备的两大功能：高效、可靠的网络通信能力；多种网络服务功能，如远程作业录入并进行处理的服务功能、文件传输服务功能、远程打印服务功能等。

（3）常用的局域网 NOS 有 NetWare、Windows、UNIX、Linux 等。

（4）NetWare 服务器对无盘站和游戏的支持较好，常用于教学网和游戏厅。微软的网络操作系统一般只是用在中、低档服务器中，高端服务器通常采用 UNIX、Linux 或 Solairs 等非 Windows 操作系统。

（5）Windows 的组网方式包括工作组模式、C/S 模式和域模式。

（6）Active Directory 是 Windows 2003/2008 操作系统平台的核心组件。

（7）常见的 Windows 文件系统有 FAT、FAT32、NTFS 等。

思 考 题

一、填空题

1．网络操作系统的发展经历了从对等结构向_____结构演变的过程。

2．网络操作系统的基本任务是：屏蔽本地资源与网络资源的差异性，为用户提供各种基本网络服务功能，完成网络_____的管理，并提供网络系统的安全性服务。

3. 网络操作系统为支持分布式服务，提出了一种新的网络资源管理机制，即分布式_____管理机制。

4．尽管 Windows NT 操作系统的版本不断变化，但是从它的网络操作与系统应用角度来看，有两个概念是始终没有变的，即工作组模型与_____模型。

5．Linux 以其低价位、_____、配置相对简单而受到用户的欢迎。

二、单项选择题

1．在下列任务中，_____是网络操作系统的基本任务。

（1）屏蔽本地资源与网络资源之间的差异。

（2）为用户提供基本的网络服务功能。

（3）管理网络系统的共享资源。

（4）提供网络系统的安全服务。

A．（1）和（2）　　B．（1）和（3）

C．（1）、（2）和（3）　　D．全部

2．在以下关于网络操作系统基本任务的描述中，错误的是_____。

A．屏蔽本地资源与网络资源的差异性

B．为用户提供各种基本网络服务功能

C．提供各种防攻击安全服务

D．完成网络共享系统资源的管理

三、问答题

1．什么是网络操作系统？它们应具备哪些功能？

2．试对 NetWare、Windows NT、UNIX、Linux 这几种操作系统做一比较。

3．Windows 网络主要有哪几种模式。

实训 2——Windows Server 2003 的安装和常见的网络命令使用

一、实训目的

1．了解 Windows Server 2003 的安装过程。

2．熟悉常见的网络命令的使用。

二、实训环境

某公司有一台服务器，要求在其上安装 Windows Server 2003 操作系统，并测试网络的基本功能是否正常。

三、实训内容

1．确保在计算机 BIOS 设置中使光驱第一个启动。

2．为系统分区分配适当的容量，并将这个分区格式化为 NTFS。

3．在系统分区上安装 Windows Server 2003。

4．几个 Windows 网络命令的使用。

四、实训步骤

1．安装 Windows Server 2003 操作系统。

（1）在计算机 BIOS 设置中，将光驱设置为第一个启动。

（2）在光驱中放入 Windows Server 2003 企业版安装光盘，重新启动计算机。

（3）根据提示，将系统分区格式化为 NTFS。

（4）完成 Windows Server 2003 企业版的安装。

2．网络命令的使用。

（1）启动网络中的所有计算机，并在本机 MS-DOS 提示符下输入“PING 网络中某台机器名或 IP 地址”（可以通过查看相邻计算机机器名称或者 IP 地址的方法），查看连通情况。

（2）在本机 MS-DOS 提示符下输入“ipconfig/all”，记录命令运行结果，记录本机 IP 地址、DNS 服务器地址以及本机对应的 MAC 地址。

（3）在本机 MS-DOS 提示符下输入“netstat -a”命令，显示出本机所有开放的端口号，并记录结果。

（4）在本机 MS-DOS 提示符下输入“nbtstat -a 某台计算机的 IP 地址”命令，显示对方机器的计算机名、所在组或域名、当前用户名，记录结果。

（5）在 MS-DOS 提示符下输入“ARP-a”，以用于查看高速缓存中的所有 IP 地址和 MAC 地址的对应项目。

（6）在 MS-DOS 提示符下输入“tracert www.163.com”网络命令，查看经过多少路由才可以到达网易网站，并做记录。另外寻找 2～3 个网站，做 tracert 实训，并记录。

（7）在 MS S-DOS 提示符下输入“nslookup”网络命令，显示本机的 DNS 服务器地址并记录，然后在“＞”提示符下输入“www.163.com”，最后回车，查看经过 DNS 服务器解析后的地址并记录。自己找两个其他网址，重复上述步骤并记录。

（8）在本机 MS-DOS 提示符下输入“net view 某机的 IP 地址”以显示该机上的共享资源；在本机 MS-DOS 提示符下输入“net use K：\\某机的 IP 地址\MUSIC（music 为共享目录，可以提前设置）”，将这个 IP 地址机上的 MUSIC 共享目录映射为本地的 K 盘；在本机 MS-DOS 提示符下输入“net share”显示本机共享资源；在本机 MS-DOS 提示符下输入“net share c$ /d”以删除共享；增加一个共享：c:\net share music=e:\ music /users:1，这样 music 共享成功，同时限制链接用户数为 1 人。

（9）通过搜索引擎，输入“网络命令帮助”内容，搜索上述网络命令的帮助信息。根据帮助信息重复做上述实验，以加深实验效果。

实训 3——Windows Server 2003 活动目录的安装

一、实训目的

1．在 Windows Server 2003 上实现域控制服务器。

2．熟悉 Active Directory 的配置与管理。

二、实训环境

一台安装了 Windows Server 2003 的独立服务器，NTFS 分区。

三、实训内容

1．安装前的准备如下。

（1）文件系统和网络协议：活动目录必须安装在 NTFS 分区，因此 Windows Server 2003 所在的分区必须是 NTFS 文件系统；同时，计算机上必须正确安装了网卡驱动程序，并启用了 TCP/IP 协议。

（2）域结构规划：活动目录可包含多个域，只有合理地规划目录结构，才能充分发挥活动目录的优越性。选择根域最为关键，在本次实训中，我们使用 cec.net 作为根域名。

（3）至少有一个 DNS 服务器：在 TCP/IP 网络中，DNS 用于解决计算机名字和 IP 地址的映射关系。活动目录和 DNS 密不可分，它使用 DNS 服务器来登记域控制器的 IP、各种资源的定位等，因此在一个域林中至少有一个 DNS 服务器。Windows Server 2003 中的域也是采用 DNS 的格式来命名的。在本次实训中，只需要将 DNS 服务安装在服务器上即可，具体配置将在第 5 章介绍。

2．安装活动目录。

四、实训步骤

1．首先确认“本地连接”属性 TCP/IP 首选 DNS 是否指向了本机（本例为 192.168.1.2），然后在“管理您的服务器”窗口中，单击“添加或删除角色”，启动“配置您的服务器向导”，单击“下一步”按钮检测所有的设备、操作系统，并搜索网络连接。搜索完成，在弹出“配置选项”窗口中，选择“自定义配置”单选钮。

2．单击“下一步”按钮，在“服务器角色”列表框中列出了所有可以安装的服务器，选择“域控制器”选项，将该计算机设置为域控制器，并同时安装活动目录。

3．单击“下一步”按钮，显示“选择总结”窗口，此处说明将“运行 Active Directory 安装向导来将此服务器设置成域服务器”，直接单击“下一步”按钮，启动“Active Directory 安装向导”窗口。

4．单击“下一步”按钮，弹出“操作系统兼容性”窗口，此处对安装活动目录以后的情况进行了简单说明。

5．单击“下一步”按钮，弹出“域控制器类型”窗口，选择此服务器要担任的角色。如果当前服务器未曾安装过 Active Directory，并且要保留这个服务器上的所有账户，则建议选择“新域的域控制器”选项。

6．选择“新域的域控制器”选项后，单击“下一步”按钮，弹出“创建一个新域”窗口。如果以前曾在该服务器上安装过 Active Directory，可以选择“在现有的域树中的子域”或“在现有的林中的域树”选项。如果是第一次安装，则建议选择“在新林中的域”选项。

7．选择“在新林中的域”选项后，单击“下一步”按钮，弹出“新的域名”窗口，在“新域的 DNS 全名”文本框中输入该服务器的 DNS 全名：“cec.net”。如果尚未申请正式域名，也应当输入拟申请的域名。

注意：此处的域名必须与网络 DNS 服务的域名相对应。

8．单击“下一步”按钮，弹出“NetBIOS 域名”窗口，在“域 NetBIOS 名”文本框中，显示该服务器的新域的 NetBIOS 名称。NetBIOS 名称的意义是，让使用其他早期 Windows 版本的用户可以识别新域。

9．单击“下一步”按钮，弹出“数据库和日志文件文件夹”窗口，Active Directory 数据库默认位于系统盘 Windows 文件夹下；也可以单击“浏览”按钮更改为其他路径，建议不做更改。其中，数据库文件夹用来存储互动目录数据库，而日志文件夹用来存储活动目录的变化日志，以便于日常管理和维护。

10. 单击“下一步”按钮，弹出“共享的系统卷”窗口，用来指定作为系统卷共享的 SYSVOL 文件夹的位置，该文件夹必须在 NTFS 格式的分区中，默认为在系统盘 Windows 文件夹下，建议不做修改。

11．单击“下一步”按钮，弹出的“DNS 注册诊断”窗口，系统会对该服务器进行 DNS 诊断测试，并显示出诊断结果，直接选择第 2 个单选项即可。如果出现其他提示信息，也可以另外选择合适的选项。

12. 单击“下一步”按钮，弹出“权限”窗口，选择“只与 Windows 2003 或 Windows Server 2003 操作系统兼容的权限”选项。

13．单击“下一步”按钮，弹出“目录服务还原模式的管理员密码”窗口。目录还原时不在 Windows 状态下，而是在“目录服务还原模式”状态下，需要输入单独的密码才能进入。因为该密码和管理员密码可能不同，所以管理员一定要牢记该密码。在“还原框密码”和“确认密码”文本框中分别输入相同的密码，密码可以为空。

14．单击“下一步”按钮，弹出“摘要”窗口，列出前面所有的配置信息。如果认为配置有错误，可以单击“上一步”按钮返回检查并修改。

15．如果确认无须更改，可以单击“下一步”按钮开始安装。因为这个过程需要几分钟或更长的时间，所以要耐心等待，完成后会弹出提示窗口，表示至此活动目录安装成功。

活动目录安装之后，必须重新启动计算机，活动目录才会有效。

第 4 章　计算机局域网组网技术

本章要点

在当今计算机网络技术中，局域网技术已经占据十分重要的地位。本章将从计算机局域网的特点、拓扑结构、传输介质和分类入手，介绍典型局域网的介质访问控制方式、以太网技术、无线局域网技术和局域网组网实例等内容。

本章目标

- 了解局域网的基本概念、特点和分类
- 了解局域网的拓扑结构、传输介质
- 掌握常用局域网的介质访问控制方法
- 掌握传统以太网和快速以太网的组成
- 了解千兆位以太网和万兆位以太网的类型和应用
- 掌握交换式以太网的基本工作原理
- 了解虚拟局域网的特点和应用
- 了解无线局域网的基本工作原理

4.1　局域网概述

局域网（Local Area Network，LAN），是一种在有限的地理范围内将大量 PC 及各种设备互连在一起实现数据传输和资源共享的计算机网络。在当今的计算机网络技术中，局域网技术已经占据十分重要的地位。

4.1.1　局域网的主要特点

局域网具有以下主要特点：

（1）覆盖范围小。一般为数百米至数公里，如一所学校、一个企业、一个工厂、一幢大楼，甚至是一个房间。

（2）数据传输速率高。通常为 10～100Mbps，目前速率高达 1Gbps 的局域网也已经广泛使用。可交换各类数字和非数字（如语音、图像、视频等）信息。

（3）误码率低。局域网通常采用短距离基带传输，可以使用高质量的传输介质，从而提高数据传输质量。误码率一般为 10^{-11}～10^{-8}。

（4）以 PC 为主体，包括终端及各种外设，网中一般不设中央主机系统。

（5）建网成本低、周期短。由于网络区域有限，所用通信线路短，网络设备相对较少，从而降低了网络成本，缩短了建网周期。

（6）协议简单、结构灵活、便于管理和扩充。

局域网的特性主要涉及拓扑结构、传输介质和介质访问控制等三项技术问题，其中最重

要的是介质访问控制。

4.1.2 局域网的拓扑结构

网络的拓扑结构对网络性能有很大的影响。局域网常用的拓扑结构有总线形、环形、星形三种。

（1）总线形拓扑结构是一种基于公共主干信道的广播式拓扑结构。总线形拓扑结构的可靠性高、扩充性能好、通信电缆长度短、成本低，是用来实现局域网的最通用的拓扑结构，如由同轴电缆做总线的 10Base-5 和 10Base-2 以太网就是典型的总线形拓扑结构。总线形拓扑结构的缺点是，若主干电缆某处发生故障，则整个网络将瘫痪；另外，当网上站点较多时，会因数据冲突增多而使效率降低。

（2）环形拓扑结构是一种基于公共环路的拓扑形式，其控制方式可集中于某一节点，但一般大都将控制分布于环上各个节点上，其信息流一般是单向的，路由选择简单。环形拓扑结构的控制简单、信道利用率高、通信电缆长度短、不存在数据冲突问题，在局域网中的应用较广泛，典型实例有 IBM 令牌环和 FDDI。环形拓扑结构的缺点是，对节点接口和传输线的要求较高，一旦接口发生故障，则可能导致整个网络不能正常工作。

（3）星形拓扑结构是一种集中控制的拓扑形式。星形拓扑结构简单、实现容易、信息延迟确定。缺点是通信电缆总长度长、传输介质不能共享。常见的星形局域网是基于集线器和交换机的以太网。

4.1.3 局域网的传输介质

局域网中常用的传输介质有双绞线、同轴电缆和光纤，还有微波和红外等。

（1）双绞线介质有非屏蔽双绞线（UTP）和屏蔽双绞线（STP）。其中，UTP 在共享介质局域网和交换式局域网中均得到广泛应用。

（2）同轴电缆有基带同轴电缆和宽带同轴电缆之分，分别用于基带系统和宽带系统。基带同轴电缆在几千米距离内可提供 10Mbps 的传输速率；宽带同轴电缆与有线电视网的传输介质相同，可提供 50Mbps 的传输速率。

（3）光纤有单模光纤和多模光纤。在局域网领域中，主要用于较大范围的局域网和基于高速交换机的高速局域网。

（4）在某些有移动性要求、不便采用有线介质的场合中，可以采用微波、红外线等传输介质连接成无线局域网。

4.1.4 局域网的分类

局域网可以按多种方法进行分类，常用的有如下几种。

（1）按拓扑结构分，可分为星形局域网、总线形局域网和环形局域网。目前常用的是总线形和星形局域网。

（2）按传输介质分，可分为双绞线局域网、同轴电缆局域网、光纤局域网和无线局域网。目前使用最多的是双绞线局域网和光纤局域网。

（3）按介质访问控制方式分，可分为以太网、令牌环网和令牌总线网等。目前使用最多的是以太网。

（4）按传输信号来分，可分为基带局域网和宽带局域网。基带局域网传输数字信号，信

号占用整个频带，传输距离较短；宽带局域网可传输模拟信号，距离较远，可达几千米以上。目前使用最多的是基带局域网。

4.2 局域网介质访问控制

介质访问控制方法，对网络性起着十分重要的作用。不论是总线形网、环形网还是星形网，都是在同一传输介质中连接了多个站，而局域网中所有的站都是对等的，任何一个站都可以和其他站通信，这就需要有一种仲裁方式来控制各站使用介质的方法，这就是所谓的介质访问控制方法。介质访问控制方法是确保对网络中各个节点进行有序访问的一种方法。在共享式局域网的实现过程中，可以采用不同的方法对其共享介质进行控制。常用的介质访问方法包括：

（1）带冲突检测的载波侦听多路访问（CSMA/CD）方法。

（2）令牌总线（Token Bus）方法。

（3）令牌环（Token Ring）方法。

目前最流行的局域网——以太网（Ethernet）使用的就是 CSMA/CD 方法，而 FDDI 网则使用令牌环方法。

4.2.1 CSMA/CD

1．什么是CSMA/CD

以太网的核心技术是随机争用型介质访问控制方法，即带冲突检测的载波侦听多路访问（CSMA/CD，Carrier Sense Multiple Access with Collision Detection）方法，它是目前占据市场份额最大的局域网技术。IEEE 802.3 标准规定了 CSMA/CD 方法和物理层技术规范。CSMA/CD 采用分布式控制方法，接入总线的各个节点通过竞争的方式，获得总线的使用权。只有获得使用权的节点才可以向总线发送信息帧，该信息帧将被接入总线的所有节点感知。

（1）载波侦听：发送节点在发送信息帧之前，必须侦听介质是否处于空闲状态。

（2）多路访问：具有两种含义，既表示多个节点可以同时访问介质，也表示一个节点发送的信息帧可以被多个节点所接收。

（3）冲突检测：发送节点在发出信息帧的同时，还必须侦听介质，判断是否发生冲突（同一时刻，有无其他节点也在发送信息帧）。

2．CSMA/CD的发送过程

CSMA/CD 的发送流程可以概括为“先听后发，边听边发，冲突停止，延迟重发”16 个字。图 4.1 是 CSMA/CD 的发送工作流程。

在 CSMA/CD 方式中，发送站检测通信信道中的载波信号。如果检测到载波信号，则说明没有其他站在发送数据，或者信道上没有数据，该站可以发送；否则，说明信道上有数据，等待一定时间后再次试探，直到能够发送数据为止。

当信号在电缆中传送时，每个站都能检测到。所有的站均检查数据帧中的地址字段，并依此判断是接收该帧还是忽略该帧。

由于数据在网中的传输需要时间，某些位置靠后的站就侦听不到任何消息，而此时信道中又确实有信号传送，因此就会发生冲突。这时就用到了冲突检测，每个发送站同时侦听自己的信号。如果该信号出现错误，发送站再发送一个干扰信息加强冲突。任何站侦听到干扰

信号后，均停止一段时间再去试探。这一时间由网卡中的算法来决定。

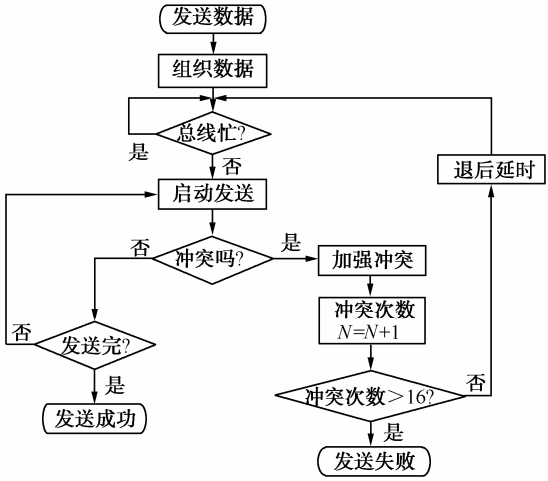


图 4.1　CSMA/CD 的发送工作流程

3．CSMA/CD的接收过程

在接收过程中，以太网中的各节点同样需要监测信道的状态。如果发现信号畸变，则说明信道中有两个或多个节点同时发送数据，有冲突发生，这时必须停止接收，并将接收到的数据丢弃。如果在整个接收过程中没有发生冲突，则接收节点在收到一个完整的数据后，可对数据进行接收处理。图 4.2 是 CSMA/CD 的接收工作流程。

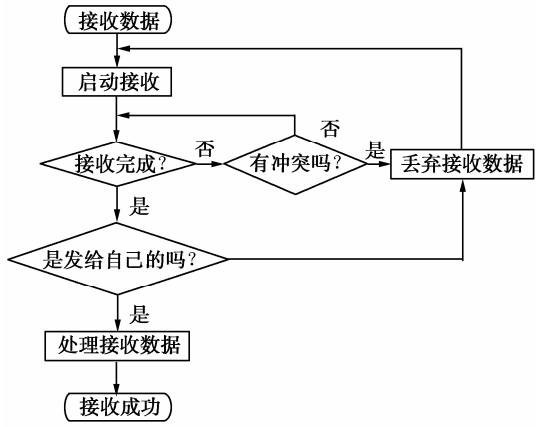


图 4.2　CSMA/CD 的接收工作流程

4．CSMA/CD的优、缺点

CSMA/CD 的优点是：每个节点都处于平等地位去竞争传输介质，实现算法简单；网络维护方便，增删节点容易；负载较少时，要发送信息的节点可以“立即获得介质的访问权，执行发送操作，效率较高。该方法的缺点是：不具有某些场合要求的优先权；负载重时，容易发生冲突，使传输效果和有效带宽大为降低，不确定的等待时间和延迟可能在过程控制应用中产生严重问题。

4.2.2 令牌环与FDDI

1．令牌环

令牌环（Token Ring）介质访问控制技术最早开始于 1969 年贝尔实验室的 Newhall 环网，最有影响的令牌环网是 IBM 公司的 IBM 令牌环。IEEE 802.5 就是在 IBM 令牌环基础上发展形成的令牌环标准。令牌环网的传输介质可以使用双绞线、同轴电缆和光纤。

在令牌环网中，节点通过环接口连接成物理上的环形结构，图 4.3 给出令牌环的基本工作过程。

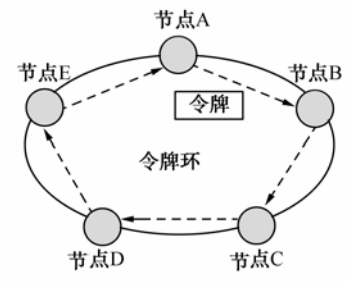


图 4.3　令牌环的基本工作过程

所谓令牌就是一个具有特殊格式的帧，通常是一个 8 位的帧，它一直在环上按一个方向从一个节点到另一个节点流动。只有获得令牌的站才有权发送信息，如果一个站无信息可传送，它就把令牌交给下一个站。令牌有“闲”和“忙”两个状态，开始时为闲。一个节点有数据要发送，必须等待空闲令牌的到来；检测到空闲令牌的到来，便将它截获下来，置令牌的状态为“忙”，并把要传送的数据等字段加上去，令其继续往前传送；每到一个站点，该站点的转发器便将帧内的目的地址与本站的地址进行比较，如果两个地址符合，则复制该帧，并在帧中置入“已收到”标志，然后让帧继续传送；当传回发源站点时，若没有检查到“已收到”标志则继续发送当前帧；若检查到“已收到”的标志就停止传送，撤销所发送的数据帧并立即生成一个新的令牌发送到环上（这时还有数据就继续发送，否则生成空闲令牌）。这种由发送站回收令牌的策略具有广播性，允许多个站点接收同一数据帧。

令牌传送方式是一种无冲突的介质共享方式，常用于负载较重、通信量较大的网络，地理范围也比以太网大。不像以太网那样，随着负荷的增加和冲突增多，网络效率急剧下降。令牌环网的缺点是：令牌环维护复杂，实现较困难。为了防止令牌的损坏、丢失或出现两个甚至多个令牌等错误，网络必须有错误检测能力和恢复机制等。此外，令牌环网采用了集中管理方式，而该网络控制站一旦出现问题便会造成一些麻烦。

2．FDDI

光纤分布式数据接口（Fiber Distributed Data Interface，FDDI）是在令牌环网的基础上发展起来的，它是一个技术规范，描述了一个以光纤为介质的高速（100Mbps）令牌环网。FDDI 为各种网络提供高速连接。

1）FDDI的拓扑结构

FDDI 是使用双环结构的令牌传递系统。FDDI 网络的网络信息流量由类似的两条流组成，两条流以相反的方向绕着两个互逆环流动。其中一个环称为主环逆时钟传送数据，另一个环称为从环，顺时针传送数据。通常情况下，网络数据信息只在主环上流动。如果主环发生故

障，FDDI 自动重新配置网络，信息可以沿反方向流到从环上去，如图 4.4（a）所示。

双环拓扑结构的优点之一是冗余，一个环用于信息传送，另一环用于备份。如果出现问题，其中主环断路，从环替代。若两者同时在一点断路，例如起火或出现电缆管道故障，两个环可连成单一的环，如图 4.4（b）所示，长度为原来的 2 倍。

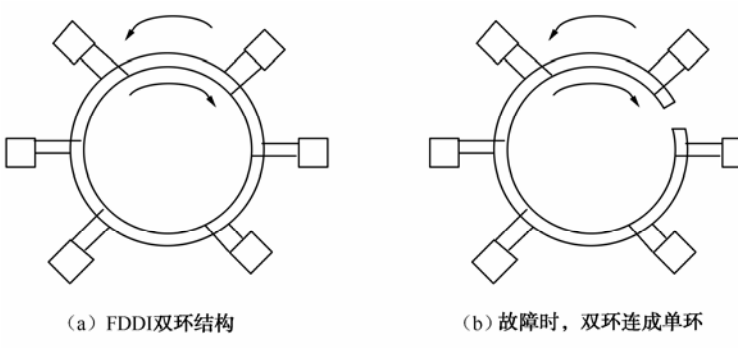


图 4.4　FDDI

2）FDDI的工作原理

FDDI 采用令牌传递的方法，实现对介质的访问控制。这一点与令牌环类似。不同的是，在令牌环中，数据帧在环路上绕行一周回到发送站点后，发送结点才释放令牌，在此期间，环路上的其他结点无法获得令牌，不能发送数据。在令牌环网中，环路上只有一个数据帧在流动。在 FDDI 中，发送数据的站点在截获令牌后，可以发送一个或多个数据帧，当数据发送完毕或规定时间用完时，则立即释放令牌，而不管发出的数据帧是否绕行一周回到发送站点。这样，在数据帧还没有回到发送它的站点且被清除之前，其他站点有可能截获令牌，并且发送数据帧。在 FDDI 的环路中可能同时有多个站点发出的数据帧在流动。这样提高了信道的利用率，增加了网络系统的吞吐量。

在正常情况下，FDDI 中主要存在以下一些操作。

（1）传递令牌。在没有数据传送时，令牌一直在环路中绕行。某个站点如果没有数据要发送，则转发令牌。

（2）发送数据。如果某个站点需要发送数据，当令牌传到该站点时，不转发令牌，而是发送数据。可以一次发送多个数据帧。当数据发送完毕或到时，则停止发送，并立即释放令牌。

（3）转发数据帧。每个站点侦听经过的数据帧，如果不属于自己，则转发出去。

（4）接收数据帧。当站点发现经过的数据帧属于自己，就复制下来，然后转发出去。

（5）清除数据帧。发送站点与其他站点一样，随时侦听经过的帧，发现是自己发出的帧就停止转发。

3）FDDI的特点

FDDI 作为高速局域网介质访问控制标准，与 IEEE 802.5 标准相似，有如下特点。

（1）使用基于 IEEE 802.5 的单令牌的环网介质访问控制 MAC 协议。

（2）使用 IEEE 802.2LLC 协议，与符合 IEEE 802 标准的局域网兼容。

（3）数据传输速率为 100Mbps，连网节点数不多于 1000，环路长度为 200km。

（4）可以使用双环结构，具有容错能力。

（5）可以使用多模或单模光纤。

（6）具有动态分配带宽的能力，能支持同步和异步数据传输。

4）FDDI的应用环境

（1）计算机机房网（后端网络），用于计算机机房中大型计算机与高速外设之间的连接，以及对可靠性、传输速度与系统容错要求较高的环境。

（2）办公室或建筑物群的主干网（前端网络），用于连接大量的小型机、工作站、个人计算机与各种外设。

（3）校园网的主干网，用于连接分布在校园中各个建筑物中的小型机、服务器、工作站、个人计算机以及多个局域网。

（4）多校园的主干网，用于连接地理位置相距几公里的多个校园网、企业网，成为一个区域性的互连多个校园网、企业网的主干网。

4.2.3 令牌总线

IEEE 802.4 标准定义了令牌总线（Token Bus）的介质访问控制方法与相应的物理规范。

从物理拓扑上看，令牌总线网为总线结构；从逻辑上看，所有主机形成一个逻辑环。令牌总线网的物理和逻辑结构如图 4.5 所示。

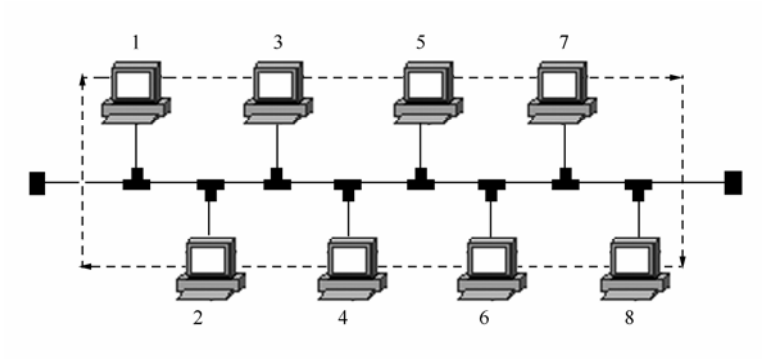


图 4.5　令牌总线网的物理和逻辑结构

连接到总线上的每台机器都有自己的一个站号，站号从大到小排队形成一个逻辑环，每个站都知道自己左边和右边的站地址。逻辑环初始化后，站号最大的站发出一个令牌给它右边的站，这个令牌就在逻辑环上传送，只有得到令牌的站才有权发送帧。因为任一时刻只有一个站掌握有令牌，不会有多个站同时向总线上发信息，也就不会产生冲突。

令牌总线的传输介质使用的是 75Ω 电视用宽带同轴电缆，传输速率为 1～10Mbps。

4.3　以太网技术

以太网是应用最为广泛的局域网，包括传统以太网（10Mbps）、快速以太网（100Mbps）、千兆（1000 Mbps）以太网和万兆（10Gbps）以太网，它们都符合 IEEE 802.3 系列标准规范。以太网采用的传输介质有同轴电缆、双绞线、光缆等，网络速度从 10Mbps、100Mbps 到 1000Mbps，介质访问控制方法是 CSMA/CD。

4.3.1 以太网的产生与发展

1975 年，美国 Xerox（施乐）公司成功研制了以太网（Ethernet），以历史上表示传播电磁波的以太（Ether）命名该网络。

1980 年 9 月，Xerox、DEC 和 Intel 三家公司合作第一次公布了以太网的物理层、数据链路层规范；1981 年 11 月公布了 Ethernet V2.0 规范。

1982 年 12 月，IEEE 在 Ethernet V2.0 规范的基础上制定了 IEEE 802.3 标准。IEEE 802.3 标准的出现，标志着符合国际标准、具有高度互通性的以太网产品的面世。IEEE 802.3 标准规定以太网是以 10Mbps 的速度运行，采用 CSMA/CD 介质访问控制方式在共享介质上传输数据的技术。以太网产品在局域网中得到了广泛的应用。

1990 年，为了提高网络带宽，一种能同时提供多条传输路径的以太网设备出现了，这就是以太网交换机，它标志着以太网从共享时代进入了交换时代。以太网交换机是一个多端口网络设备，不仅将竞争信道的端口数减少到 2 个，还支持在几个端口同时传输数据，因此，它的出现，改变了共享式集线器多个端口共享 10Mbps 带宽的局面，显著地提高了网络的整体带宽。

1993 年，全双工以太网的出现，又改变了以太网半双工的工作模式，不仅使以太网的传输速度翻了一番，而且彻底解决了多个端口的信道竞争。

1995 年 3 月，IEEE 802.3u 规范的通过，标志着以 100Mbps 的速度运行的快速以太网时代的来临。

1998 年 6 月，IEEE 802.3z 规范的通过，又使以太网进入了高速网络的行列，运行速度达到了 1000Mbps（即 1Gbps）。以快速以太网连接桌面、高速以太网连接核心的高速局域网的现在已经广泛使用。

4.3.2 传统以太网技术

传统以太网技术是早期广泛应用的一类局域网技术，其典型速率是 10Mbps。

1．10Mbps以太网体系结构

IEEE 802.3 以太网体系结构包括 MAC 子层和物理层。物理层又分为物理信令（PLS）和物理介质连接（PMA）两个子层，并根据物理层的两个子层是否在同一个设备上实现。10Mbps 以太网体系结构示意图如 4.6 所示。

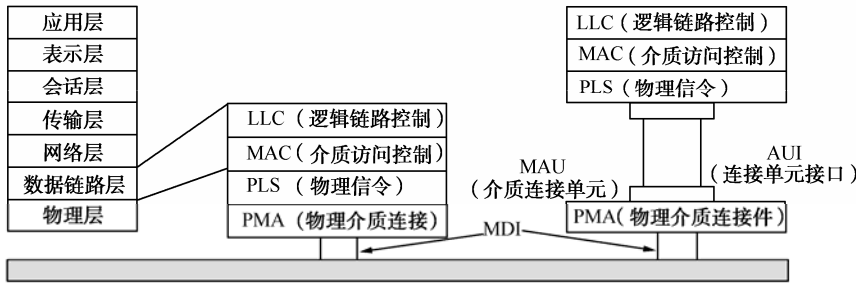


图 4.6　10 Mbps 以太网体系结构示意图

PLS 子层向 MAC 子层提供服务，它规定了 MAC 子层与物理层的界面，是与传输介质无

关的物理层规范。在发送比特流时，PLS 子层负责对比特流进行曼彻斯特编码。在接收时，负责进行曼彻斯特解码。另外，PLS 子层还负责完成载波侦听功能。PMA 子层向 PLS 子层提供服务，它负责向介质上发送比特信号和从介质上接收比特信号，并完成冲突检测功能。IEEE 802.3 标准规定，PLS 子层和 PMA 子层可以在也可以不在同一个设备中实现。比如，标准以太网 10Base-5 是在网卡中实现 PLS 功能，在外部接收器中实现 PMA 功能的，所以在 10Base-5 以太网中，需要使用收发器电缆将外部收发器和网络站点连接起来。

MAC 子层的核心协议是 CSMA/CD，IEEE 802.3 帧结构如图 4.7 所示。

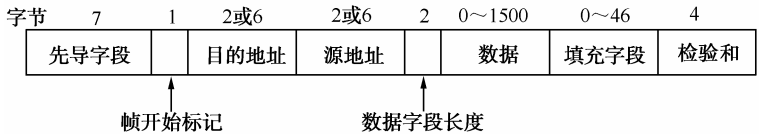


图 4.7　IEEE 802.3 帧结构

其中，7 个字节的先导字段是接收方与发送方时钟同步用的，它的每个字节的内容都是 10101010。一个字节的帧开始标志，表示一个帧的开始，内容为 10101011。随后是两个地址段：源地址和目的地址。目的地址可以是单个的物理地址，也可以是一组地址（多点广播）。当地址的最高位为 0 时，是普通地址；为 1 时，是组地址。2 个字节的数据字段长度标志数据段中的字节数。数据字段就是 LLC 数据帧，如果帧的数据部分少于 46 个字节，则用填充字段，以达到要求的最短长度。

2．MAC地址

连入网络的每台计算机或终端都有一个惟一的物理地址，这个物理地址存储在网络接口卡（Network Interface Card，NIC）中，通常称为介质访问控制地址（Media Access Control Address），或者简单地称为 MAC 地址。在网络中，网络接口卡将设备连接到传输介质中，每个网络接口卡都有一个惟一的 MAC 地址，它位于 OSI 参考模型的数据链路层。

当源主机向网络发送数据时，它带有目的主机的 MAC 地址。当以太网中的节点正确收到该数据后，它们检查数据中包含的目的主机 MAC 地址是否与自己网卡上的 MAC 地址相符。如果不符，网卡就忽略该数据。如果相符，网卡就复制该数据，并将该数据送往数据链路层作进一步处理。

以太网的 MAC 地址长度为 48b。为了方便起见，通常使用十六进制数书写（如 00-50-56-C0-00-98）。为了保证 MAC 地址的惟一性，世界上有一个专门的组织负责为网卡的生产厂家分配 MAC 地址。

3．10 Mbps以太网组网方式

IEEE 802.3 支持的物理层介质和配置方式有多种，是由一组协议组成的。每一种实现方案都有一个名称代号，由以下三部分组成：

<数据传输率（Mbps）><信号方式><最大段长度（百米）或介质类型>

例如 10Base-5、10Base-2、100Base-T 等。这里，最前面的数字指传输速率，如 10 为 10 Mbps，100 为 100 Mbps；中间的 Base 指基带传输；最后若是数字，则表示最大传输距离，如 5 是指最大传输距离为 500m，2 指最大传输距离为 200m；若是字母，则第一个表示介质类型，如 F 表示采用光纤介质，T 表示采用双绞线；第二个字母表示工作方式，如 X 表示全双工方式工作。

IEEE 802.3 中的 10Base-2、10Base-5、10Base-F 和 10Base-T 形成了一个 10Mbps 以太网标准系列，它在物理层定义了多种传输介质（粗同轴电缆、细同轴电缆、双绞线和光纤）和

多种拓扑结构（总线形、星形和混合型）。10Mbps 网络连接图如图 4.8 所示。几种传统以太网的指标和参数如表 4.1 所示。

1）10Base-2

10Base-2 表示采用 10Mbps 的基带（Baseband）传输、传输距离是 100m 的 2 倍（实际距离是 185m）。10Base-2 网络采用直径为 5mm 的细同轴电缆，经过 BNC T 型连接器将工作站连接到细同轴电缆上，构成总线结构的网络。图 4.8（a）为 10Base-2 网络连接图。

10Base-2 网络由以下几部分组成：

（1）0.2 英寸/50Ω 细同轴电缆。

（2）带有 BNC 插座的以太网网卡。

（3）BNC T 型连接器，该三通插头的中间插网卡，两端连接细同轴电缆。

（4）BNC 连接器头，用于连接细同轴电缆与 T 型连接器。

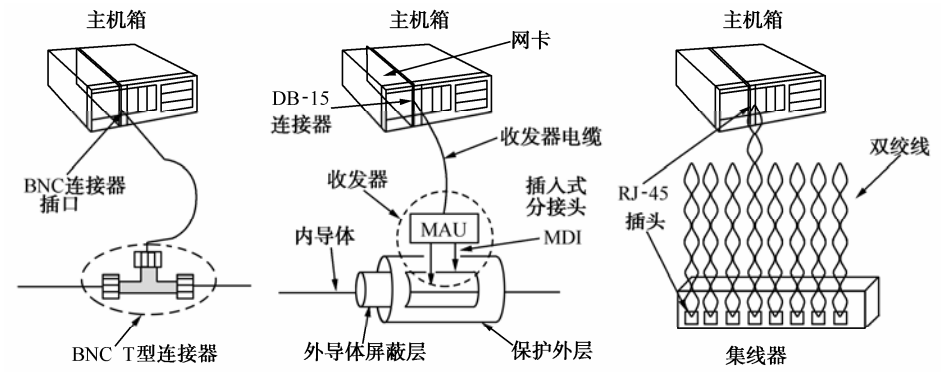
（5）BNC 圆形连接器，用于连接两端的细同轴电缆。

（6）50Ω BNC 终端匹配器，细同轴电缆两端各安装一个，用于抗干扰。

10Base-2 标准规定的网络指标和参数如表 4.1 所示。

2）10Base-5

10Base-5 通常称为粗同轴电缆以太网，采用基带传输，传输速率为 10Mbps。每个网段的电缆长度最大为 500m，通常采用黄色包层直径为 10mm 的粗同轴电缆，每隔 2.5m 有一个标记，指示接入收发器插头的位置。网卡经过 DB-15 连接器、9 线 AUI 电缆和外部收发器连接到粗同轴电缆上。粗同轴电缆的两端必须使用 50Ω 的终端匹配器，并且一端必须接地。图 4.8（b）所示为 10Base-5 网络连接图。



（a）10Base-2网络连接图　　（b）10Base-5网络连接图　　（c）10Base-T网络连接图

图 4.8　10Mbps 网络连接图

10Base-5 网络由以下几部分组成：

（1）0.4 英寸/50Ω 粗同轴电缆。

（2）带有 AUI 插座的以太网网卡。

（3）收发器，两端连接粗同轴电缆，中间经 AUI 连接器连接网卡。

（4）收发器电缆，两端带 AUI 插头，用于连接外部收发器和网卡。

（5）50Ω BNC 终端匹配器，粗同轴电缆两端各安一个，用于抗干扰。

10Base-5 标准规定的网络指标和参数如表 4.1 所示。

表 4.1　几种传统以太网的指标和参数

网络 / 参数	10Base-2	10Base-5	10Base-F	10Base-T
拓扑结构	总线形	总线形	星形	星形
传输介质	细同轴电缆	粗同轴电缆	多模光纤	3 类 UTP
连接器	BNC	AUI	SC 或 ST	RJ-45
网段最大长度	185m	500m	2000m	100m
网络最大长度	925m	2500m	2 个集线器	4 个光集线器
网站间最小距离	0.5m	2.5m		
网段最多节点数	30	100		
最多网段数	5	5	3	5

3）10Base-F

10Base-F 采用光纤介质和基带传输，传输速率为 10Mbps。由于光信号传输的特点是单向的，适合于端到端的通信。10Base-F 使用至少一对光纤（一根用于发送，另一根用于接收），一般采用多模光纤，使用 ST 或 SC 连接器。10Base-F 以太网呈星形或放射状结构。10Base-F 网络由以下几部分组成：

（1）10Base-F 光纤集线器。

（2）光网卡或光电转换器加带有 RJ-45 以太网卡。

（3）62.5/125μm 的多模光纤。

（4）SC 或 ST 光纤连接器。

10Base-F 标准规定的网络指标和参数如表 4.1 所示。

4）10Base-T

10Base-T 采用基带传输，传输速率为 10Mbps，T 表示使用双绞线作为传输介质。10Base-T 网络通过集线器（Hub）来连接各工作站，构成星形拓扑结构网络。10Base-T 网络连接如图 4.8（c）所示。

10Base-T 是目前应用最广的以太网，主要特点如下。

传输介质：直径为 0.4～0.6mm 的 2 对 3 类非屏蔽双绞线（UTP）或屏蔽双绞线（STP）。

插头：RJ-45。

最大传输距离：100m。

信号频率范围：10～20MHz。

典型产品：10Base-T 网卡和集线器（Hub）。

两个工作站之间最多允许 4 个中继器和 5 个电缆段，即 UTP 电缆的最大长度为 500m。

10Base-T 网络由以下几部分组成：

（1）10Base-T 集线器。10Base-T 集线器是 10Base-T 网络技术的核心。集线器是一个具有中继器功能的有源多口转发器，其原理是接收某一端口的信号，经过再生、整形的放大后再转发给其他端口。集线器的另一功能是网络故障自动隔离。

（2）带有 RJ-45 插座的以太网卡。

（3）3 类及 3 类以上的非屏蔽双绞线（UTP）。

（4）RJ-45 连接器。

10Base-T 标准规定的网络指标和参数如表 4.1 所示。

4.3.3 快速以太网技术

1．快速以太网的体系结构

快速以太网的传输速率比普通以太网快 10 倍，数据传输速率达到 100Mbps。快速以太网保留了传统以太网的所有特性，包括相同的数据帧格式、介质访问控制方式和组网方法，不同的只是将每个比特的发送时间由 100ns 降低到 10ns。1995 年 9 月，IEEE 802 委员会正式批准了快速以太网标准 IEEE 802.3u。IEEE 802.3u 标准在 LLC 子层使用 IEEE 802.2 标准，在 MAC 子层使用 CSMA/CD 方法，只在物理层做了一些必要的调整，定义了新的物理层标准（100Base-T）。100Base-T 快速以太网标准是对 10Base-T 标准的扩展，它保留了 10Base-T 在介质访问控制（MAC）子层的 CSMA/CD 方法与数据传输的帧格式。传输介质可以为 3、4、5 类无屏蔽双绞线和光纤。这样，快速以太网可以使原来的 10Base-T 以太网的用户在不改变网络布线、网络管理、检测技术以及网络管理软件的情况下，顺利地向 100Mbps 快速以太网升级。100Base-T 标准定义了介质专用接口（Media Independent Interface，MII），它将 MAC 子层和物理层分开，使得物理层在实现 100Mbps 速率时所使用的传输介质和信号编码方式的变化不会影响 MAC 子层。

100Mbps 以太网的协议结构如图 4.9 所示。

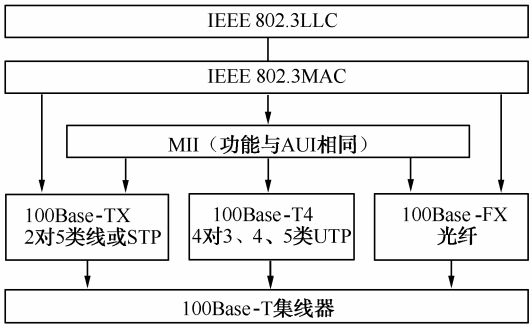


图 4.9　100Mbps 以太网的协议结构

2．快速以太网的组网方式

100Base-T 技术在网络的介质访问控制（MAC）子层上支持 100Base-TX、100Base-FX、100Base-T4 和 100Base-T2 四种介质协议。

（1）100Base-TX。使用 2 对 5 类非屏蔽双绞线或 1 类屏蔽双绞线，一对用于发送数据，另一对用于接收数据，最大网段长度为 100m，布线符合 EIA568 标准。100Base-TX 是 100Base-T 中使用最广的物理层规范。

（2）100Base-FX。使用多模（62.5 或 125μm）或单模光纤，连接器可以是 MIC/FDDI 连接器、ST 连接器或廉价的 SC 连接器；最大网段长度根据连接方式不同而变化，例如，对于多模光纤的交换机—交换机连接或交换机—网卡连接，最大允许长度为 412m，如果是全双工链路，则可达到 2000m。100Base-FX 主要用于高速主干网，或远距离连接，或有强电气干扰的环境，或要求较高、安全保密链接的环境。

（3）100Base-T4：是为了利用大量的 3 类音频级布线而设计的。它使用 4 对双绞线，3 对用于同时传送数据，第 4 对用于冲突检测时的接收信道，信号频率为 25MHz，因而可以使

用数据级 3、4 或 5 类非屏蔽双绞线，也可使用音频级 3 类线缆。最大网段长度为 100m，采用 EIA568 布线标准；由于没有专用的发送或接收线路，所以 100Base-T4 不能进行全双工操作。

（4）100Base-T2：随着数字信号处理技术和集成电路技术的发展，只用 2 对 3 类 UTP 线就可以传送 100Mbps 的数据，因而针对 100Base-T4 不能实现全双工的缺点，IEEE 开始制定 100Base-T2 标准。100Base-T2 采用 2 对音频或数据级 3、4 或 5 类 UTP 电缆，一对用于发送数据，另一对用于接收数据，可实现全双工操作；采用 RJ-45 连接器，最长网段为 100m，符合 EIA568 布线标准。

3．自动协商模式

在 100Base-T 问世以后，在以太网 RJ-45 连接器上出现的信号可能是 5 种以上不同的以太网信号（10Base-T、10Base-T 全双工、100Base-TX、100Base-TX 全双工或 100Base-T4）中的任一种。为了简化管理，IEEE 已推出了 IEEE 自动协商模式，它能使集线器和网卡知道线路另一端能有的速度，把速度自动调节到线路两端能达到的最高速度（优先的顺序为：100Base-T2 全双工、100Base-T2、100Base-TX 全双工、100Base-T4、100Base-TX、100Base-T 全双工、10Base-T）。这是增强型 10Base-T 链路一体化信号方法，并与链路一体化反向兼容。这种技术避免了由于信号不兼容可能造成的网络损坏。具有这种特性的装置仍允许人工选择可能的模式。

4.3.4　千兆以太网技术

1．千兆以太网的体系结构

1998 年 2 月，IEEE 802 委员会正式批准了千兆以太网标准 IEEE 802.3z。千兆以太网技术作为最新的高速以太网技术，给用户带来了提高核心网络的有效解决方案，这种解决方案的最大优点是继承了传统以太技术价格便宜的优点。千兆技术仍然是以太技术，它采用了与传统以太网（10Mbps）相同的帧格式、帧结构、网络协议、全/半双工工作方式、流控模式以及布线系统。由于该技术不改变传统以太网的桌面应用、操作系统，因此可与传统以太网或快速以太网（100Mbps）很好地配合工作。升级到千兆以太网不必改变网络应用程序、网管部件和网络操作系统，能够最大程度地投资保护。千兆以太网的协议结构如图 4.10 所示。

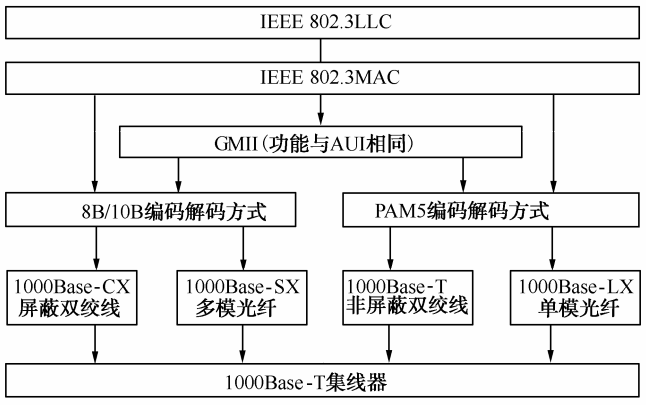


图 4.10　千兆以太网的协议结构

千兆以太网既支持铜线，也支持光纤，如表 4.2 所示。

表 4.2　千兆以太网的电缆类型

名　　称	线　　缆	最大的段距离
1000Base-SX	多模光纤（50μm、62.5μm）	550m
1000Base-LX	单模光纤（10μm）或多模光纤（50μm、62.5μm）	5000m
1000Base-CX	2 对 STP 屏蔽双绞线	25m
1000Base-T	4 对 UTP 非屏蔽双绞线	100m

2．千兆以太网的组网方式

千兆以太网技术有两个标准：IEEE 802.3z 和 IEEE 802.3ab。IEEE 802.3z 制定了光纤和短程铜线连接方案的标准，IEEE 802.3ab 制定了 5 类双绞线上较长距离连接方案的标准。

IEEE 802.3z 定义了基于光纤和短距离铜缆的 1000Base-X，采用 8B/10B 编码技术，信道传输速率为 1.25Gbps，实现 1000Mbps 传输速率。IEEE 802.3z 具有下列千兆以太网标准：

（1）1000Base-SX。1000Base-SX 是一种在收发器上使用短波激光作为信号源的媒体技术。1000Base-SX 只支持多模光纤，可以采用直径为 62.5μm 或 50μm 的多模光纤，工作波长为 770～860nm，传输距离为 220～550m。

（2）1000Base-LX。1000Base-LX 是一种在收发器上使用长波激光作为信号源的媒体技术。1000Base-LX 可以采用直径为 62.5μm 或 50μm 的多模光纤，工作波长范围为 1270～1355nm，传输距离为 550m。1000Base-LX 也支持直径为 9μm 或 10μm 的单模光纤，工作波长范围为 1270～1355nm，传输距离为 5km 左右。

（3）1000Base-CX。1000Base-CX 是使用铜缆的两种千兆以太网技术之一。1000Base-CX 采用 150Ω 屏蔽双绞线（STP），传输距离为 25m。

IEEE 802.3ab 定义基于 5 类 UTP 的 1000Base-T 标准，其目的是在 5 类 UTP 上以 1000Mbps 速率传输 100m。IEEE 802.3ab 标准的意义主要有以下两点：

（1）保护用户在 5 类 UTP 布线系统上的投资。

（2）1000Base-T 是 100Base-T 自然扩展，与 10Base-T、100Base-T 完全兼容。不过，在 5 类 UTP 上达到 1000Mbps 的传输速率需要解决 5 类 UTP 的串扰和衰减问题，因此，使得 IEEE 802.3ab 工作组的开发任务要比 IEEE 802.3z 复杂些。

3．千兆以太网的主要特点

（1）简易性：千兆以太网继承了以太网、快速以太网的简易性，因此其技术原理、安装实施和管理维护都很简单。

（2）扩展性：由于千兆以太网采用了以太网、快速以太网的基本技术，因此由 10Base-T、100Base-T 升级到千兆以太网非常容易。

（3）可靠性：由于千兆以太网保持了以太网、快速以太网的安装维护方法，采用星形网络结构，因此网络具有很高的可靠性。

（4）经济性：由于千兆以太网是 10Base-T 和 100Base-T 的继承和发展，所以降低了研究成本。由于 10Base-T 和 100Base-T 的广泛应用，作为其升级产品，千兆以太网的大量应用只是时间问题，为了争夺千兆以太网这个巨大市场，几乎所有著名网络公司都生产千兆以太网产品，因此其价格将会逐月下降。千兆以太网与 ATM 等宽带网络技术相比，其价格优势非常明显。

（5）可管理维护性：千兆以太网采用基于简单网络管理协议（SNMP）和远程网络监视

（RMON）等网络管理技术，许多厂商开发了大量的网络管理软件，使千兆以太网的集中管理和维护非常简便。

（6）广泛应用性：千兆以太网为局域主干网和城域主干网（借助单模光纤和光收发器）提供了一种高性能价格比的宽带传输交换平台，使得许多宽带应用能施展其魅力。例如，在千兆以太网上开展视频点播业务和虚拟电子商务等。

4.3.5 万兆以太网技术

千兆以太网与传统低速以太网的最大相似之处是，采用相同的以太网帧结构。万兆（10G）以太网技术与千兆以太网类似，仍然保留了以太网帧结构，通过不同的编码方式或波分复用提供 10Gbps 传输速率。就其本质而言，万兆以太网仍是以太网的一种类型。万兆以太网采用以光纤作为传输介质、以交换机作为中心的星形结构网络，可以为网络提供更大的可用带宽。万兆以太网标准 IEEE 802.3ae 于 2002 年 7 月在 IEEE 通过。

1．万兆以太网体系结构

万兆以太网的 OSI 和 IEEE 802 层次结构仍与传统以太网相同，即 OSI 层次结构包括数据链路层的一部分和物理层的全部，IEEE 802 层次结构包括 MAC 子层和物理层，但各层所具有的功能与传统以太网相比差别较大，特别是物理层更具有明显的特点。万兆以太网的体系结构如图 4.11 所示。

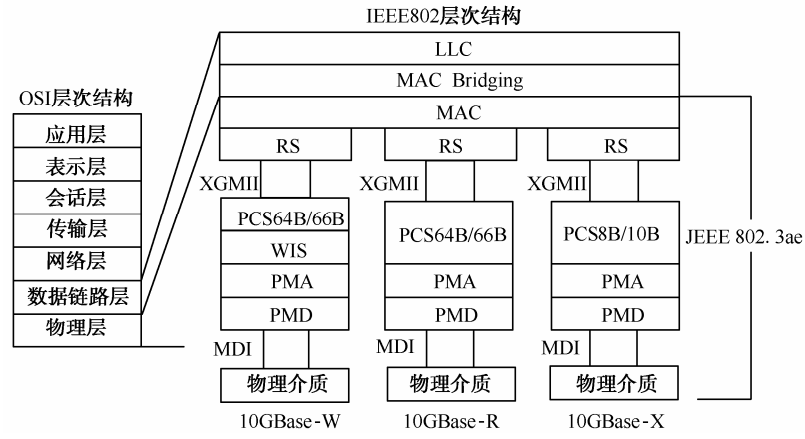


图 4.11 万兆以太网的体系结构

2．万兆以太网的分类

万兆 10G 以太网包括 10GBase-X、10GBase-R 和 10GBase-W。

10GBase-X 是一种与使用光缆的 1000Base-X 相对应的物理层结构，含有 1 个较简单的波分多路复用（WDM）器件、4 个接收器和 4 个在 1300nm 波长附近以大约 25nm 为间隔工作的激光器，每一对发送器/接收器以 3.125Gbps 速率（数据流速率为 2.5Gbps）工作。

10GBASE-R 是一种使用 64B/66B 编码（不是在千兆以太网中所用的 8B/10B）的串行接口，数据流速率为 10.000Gbps，因而产生的时钟速率为 10.3Gbps。

10GBase-W 是广域网接口，采用了 64B/ 66B 编码，与 SONET OC-192 兼容，其时钟速率为 9.953Gbps，数据流速率为 9.585Gbps。

3．万兆以太网的主要特点

万兆以太网与传统以太网比较，具有以下特点。

（1）MAC 子层和物理层实现 10Gbps 传输速率。

（2）MAC 子层的帧格式不变，并保留 IEEE 802.3 标准最小和最大帧长度。

（3）不支持共享型，只支持全双工，即只可能实现全双工交换型万兆以太网，因此万兆以太网介质的传输距离不会受到传统以太网 CSMA/CD 机理制约，而仅仅取决于介质上信号传输的有效性。

（4）支持星形局域网拓扑结构，采用点到点连接和结构化布线技术。

（5）在物理层上分别定义了局域网和广域网两种系列，并定义了适应局域网和广域网的数据传输机制。

（6）不使用双绞线，只支持多模和单模光纤，并提供连接距离的物理层技术规范。

4．万兆以太网在局域网中的应用

万兆以太网用做局域网，通常是组成主干网。例如，利用万兆以太网实现交换机到交换机、交换机到服务器以及城域网和广域网的连接。

万兆以太网在局域网中的应用如图 4.12 所示。主干线路使用万兆以太网，企业、大学、政府、数据中心和服务器群之间用万兆以太网交换机的模块分别连接。

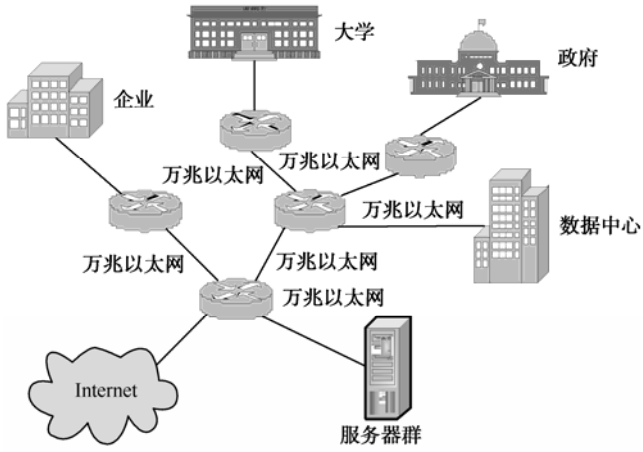


图 4.12　万兆以太网在局域网中的应用

4.3.6　交换式以太网技术

1．局域网的分段

在共享介质网络中，由于多个节点共享同一介质，整个系统处于一个冲突域范围内，对于有 *N* 个节点的网络，每个站点平均只占有系统带宽的 1/*N*。随着站点的增加，冲突的概率也会增加。解决这一问题的最初努力就是将网络分割成一些网段，使网络中的一部分站点能够并行地发送数据。把一个网络分割成子网的设备称为网桥（Bridge），也称桥接器。从另一个角度来讲，使用网桥可以将多个局域网连接起来，实现距离的扩展。

2.5.1 节已经对网桥的工作原理做了介绍，此处不再赘述。

网桥的主要用途有：

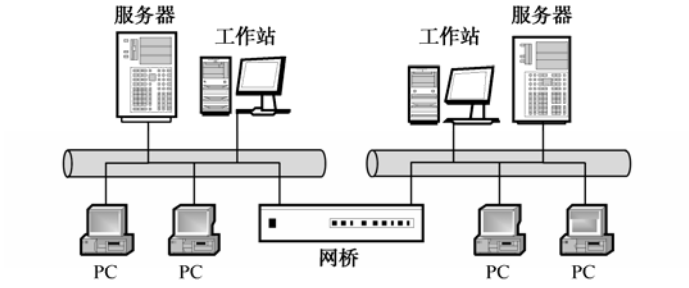
（1）用于同构型（第 3～7 层完全相同）LAN 间的连接。

（2）扩展工作站的平均占有频带。

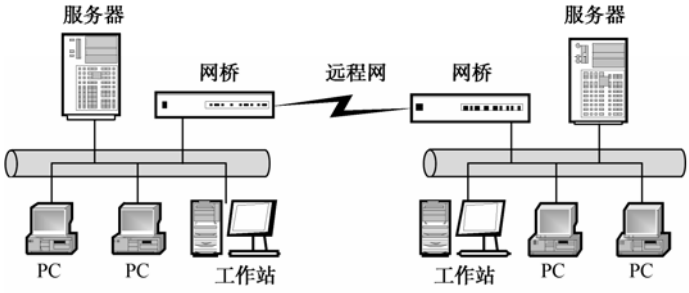
（3）扩展 LAN 的地址范围。

（4）进行网段微化，将局域网分段成几个子网，以提高信息流量和网络性能。

网桥可安装在文件服务器上，称为内桥；也可以安装在工作站上，称为外桥。图 4.13 为用网桥连接局域网和远程网的示意图。连接两个远程网时，每端各需要一个网桥。



（a）连接两个本地局域网的网桥



（b）连接两个远程局域网的网桥

图 4.13　用网桥连接局域网和远程网的示意图

2．交换式以太网

分割子网化减少了站点对总线的竞争，但在较大型的网络中，过多地分割会使得整个网络的结构和管理变得十分复杂并使成本随之增加。交换式网络则从根本上改变了共享介质工作方式，它可以通过交换机在多端口之间实现多个并发连接，实现多个节点间的并发通信，以增加带宽，改善网络性能和服务质量。图 4.14 示出一个交换式以太网结构。

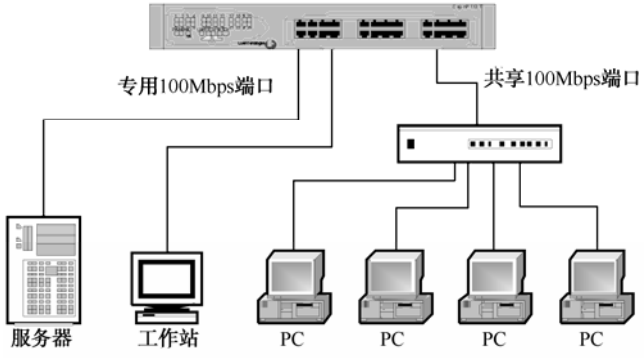


图 4.14　交换式以太网结构

4.3.7　虚拟局域网（VLAN）技术

近年来，交换局域网由于其高性能和低成本，得到了广泛的应用，同时也促进了交换技术的发展。目前，交换局域网已经基本上取代了共享介质局域网。在此基础上，一种新的网络技术——虚拟局域网（VLAN，Virtual LAN）技术呈现在人们的面前。

VLAN 是在交换技术的基础上，通过管理软件建立起来的可跨越不同物理网段、不同网络类型的站点的逻辑工作组。逻辑组中的成员不一定要在同一网段上，它们可以连接在同一个 LAN 交换机上，也可以分布在不同的 LAN 交换机上，只要这些交换机是互连的就可以。当一个站点从一个工作组迁移到另一个工作组时，只需要通过管理软件做简单的设定就可使它属于另一个逻辑工作组，而不需改变它的物理位置。

1．VLAN的特点

VLAN 具有如下特点。

（1）控制广播风暴：一个 VLAN 就是一个逻辑广播域，通过对 VLAN 的创建，隔离了广播，缩小了广播范围，可以控制广播风暴的产生。VLAN 可简化网络管理。

（2）简化网络管理：对于采用 VLAN 技术的网络来说，一个 VLAN 可以根据部门职能、对象组或者应用将不同地理位置的网络用户划分为一个逻辑网段。在不改动网络物理连接的情况下可以任意地将工作站在工作组或子网之间移动。利用虚拟网络技术，大大减轻了网络管理和维护工作的负担，降低了网络维护费用。

（3）简化网络结构：VLAN 允许网络管理员在中央节点配置和管理网络，由于网络分组比较容易，故可将部门级服务器设在网管中心，从而简化网络结构。

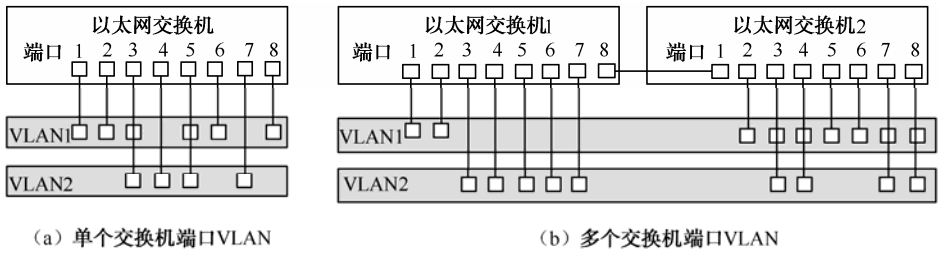
（4）提高网络安全性：通过路由访问列表和 MAC 地址分配等 VLAN 划分原则，可以控制用户访问权限和逻辑网段大小，将不同用户群划分在不同的 VLAN 中，从而提高交换式网络的整体性能和安全性。

2．VLAN的划分方法

VLAN 的划分方法很多，区别主要在对其成员资格的定义上。下面介绍 4 种通用的方法。

1）基于端口划分VLAN

基于端口划分 VLAN（端口 VLAN）分为单个交换机端口 VLAN 和多个交换机端口 VLAN，图 4.15 给出两种形式的端口 VLAN，它们都是以太网交换机。从图 4.15 可以看出，通过交换机的端口定义，可以将连接在一台交换机上的节点划分为不同的子网，也可以将连接在不同交换机上的节点划分在一个子网中。



（a）单个交换机端口VLAN　　（b）多个交换机端口VLAN

图 4.15　基于端口划分 VLAN

端口 VLAN 是早期的 VLAN 划分方法。它配置简单，但也有一定的限制：不允许不同的 VLAN 包含相同的物理网段，并且要将用户从一个端口移动到另一个端口时，必须对 VLAN

的成员进行重新配置。

2）基于MAC地址划分VLAN

基于 MAC 地址划分 VLAN（MAC VLAN）是一种基于用户的 VLAN，它用终端系统的 MAC 地址来定义 VLAN。由于 MAC 地址与硬件相关、固定于工作站的网卡之内，因此 MAC 定义的 VLAN 允许工作站移动到网络的其他物理网段中，还能保持原来的 VLAN 成员资格，因为它的 MAC 地址没有变。

MAC VLAN 的不足之处是，它要求所有用户在初始阶段必须配置到至少一个 VLAN 中；初始配置必须由人工完成，然后才可以自动跟踪用户。这对用户较多的大型网络来说工作量是非常大的。

3）基于IP地址划分VLAN

基于 IP 地址划分 VLAN 也称为网络层 VLAN。TCP/IP 协议是常用的网络协议。对于基于 TCP/IP 协议的网络，可按站点的 IP 地址定义其广播域，形成虚拟 IP 子网。虚拟子网之间通过内部路由器实现互通。

网络层 VLAN 的优点：一是它允许按照协议类型来组成 VLAN，这有利于组成基于服务或应用的 VLAN；二是用户可以随意移动工作站而无需重新配置网络地址，这对于 TCP/IP 协议用户特别有利。网络层 VLAN 的缺点是性能比较差。检查网络层地址比检查 MAC 地址要花费更多的时间，因此基于网络层地址划分 VLAN 时速度会比较慢。

4）根据IP组播划分VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN，这种划分的方法将 VLAN 扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展。这种方法不适合局域网，主要是效率不高。

4.4 无线局域网

4.4.1 无线局域网的提出

随着信息技术的发展，人们对网络通信的需求不断提高，希望不论在何时、何地与何人都能够进行数据、语音、图像等任何内容的通信。无线局域网（WLAN）是实现移动网络的关键技术之一。因此，许多研究组很早就开始为这个目标而努力，其中 IEEE 802 委员会制定的 IEEE 802.11 标准成为现行的无线局域网标准，也就是俗称的 WiFi。该标准介绍了两种工作模式：有基站模式和无基站模式。这两种模式如图 4.16 所示。

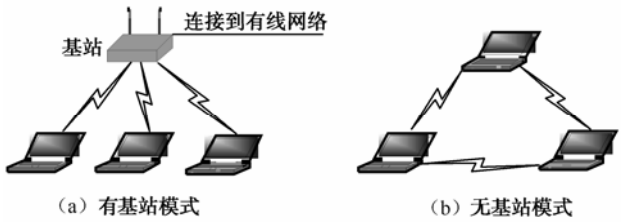


图 4.16　无线局域网的两种工作模式

在有基站模式下，所有的通信都经过基站，按照 IEEE 802.11 标准的术语，基站称为访问

点（Access Point，AP）。在无基站模式下，计算机相互之间直接发送数据，这种模式有时也称为特定网络（Ad Hoc Networking）。

WLAN 作为有线接入方式的补充，最主要的优势在于无需布线，相对于有线网络，无线局域网的组建、配置和维护较为容易。在现阶段，WLAN 的建设主要集中在对以下热点地区的覆盖上。

（1）商业楼宇：应用于租用的办公室，通过采用 WLAN 实现快速布线。

（2）信息化酒店：应用于公众活动空间，如大堂、会议室。

（3）信息中心：如展览馆信息中心、体育场所信息中心、新闻中心。

（4）机场：公共候机大厅。

（5）公众休闲场所：酒吧、咖啡厅、网吧。

4.4.2 无线局域网实现技术

无线局域网使用的是无线传输介质，按照所采用的技术可以分为三类：红外线技术、扩频技术和窄带微波技术。

1．红外线技术

红外线是按视距方式传播的，也就是说发送点可以直接看到接收点，中间没有阻挡。红外线相对于微波传输方案来说有一些明显的优点。因为红外线频谱是非常宽的，所以就有可能提供极高的数据传输速率。由于红外线与可见光的一部分特性是一致的，所以它可以被浅色物体漫反射，这样就可以用天花板反射来覆盖整个房间。红外线不会穿过墙壁或其他不透明物体，因此红外线无线局域网具有以下优点。

（1）红外线通信与微波通信相比，不易被入侵，因此提高了安全性。

（2）安装在大楼中每个房间里的红外线网络可以互不干扰，因此建立一个大的红外线网络是可行的。

（3）红外线局域网的设备相对便宜又简单。因为红外线数据基本上是用强度调制，所以红外线接收器只需测量光信号的强度，而大多数微波接收器则需测量信号的频谱或相位。

红外线局域网的缺点：室内环境中的阳光或室内照明的强光线，都会成为红外线接收器的噪声部分，因此限制了红外线局域网的应用范围。

2．扩频技术

扩展频谱技术是指发送信息带宽的一种技术，简称为扩频技术。它是一种信息传输方式，其信号所占有的频带宽度远大于所传信息必需的最小带宽。频带的扩展是通过一个独立的码序列来完成的，是用编码及调制的方法来实现的，与所传信息数据无关；在接收端也用同样的码进行相关同步接收、解扩及恢复所传信息数据。

在扩频方式中，数据基带信号的频谱被扩展几倍到几十倍后被射频发射出去。这种方式以牺牲带宽为代价，换来通信系统高抗干扰能力和高安全性，并由于单位频带内的功率降低而减小了对其他电子设备的干扰。扩频方式的 WLAN 一般采用 ISM 频段（即工业、科学、医学频段）。欧、美、日等国家各有自己的 ISM 频段范围，如美国联邦通信委员会（FCC）规定的 ISM 频段为 902～928MHz、2400～2483.5MHz、5725～5850MHz 三个频段。若发射功率以及带外辐射超过 FCC 的规定，则应当向 FCC 提出专门申请。

3．窄带微波技术

窄带微波 （Narrowband Microwave）是指使用微波无线电频带进行数据传输，其带宽刚好能容纳信号。对窄带微波方式的信号频谱不做任何扩展地直接发射出去。与扩频方式相比，

它的频带利用率高，但要选用专用频段，并需要经 FCC 批准。

4.4.3 无线局域网的基本结构模型

如图 4.17 所示，IEEE 802.11 标准规定无线局域网的最小构件是基本服务集（Basic Service Set，BSS）。

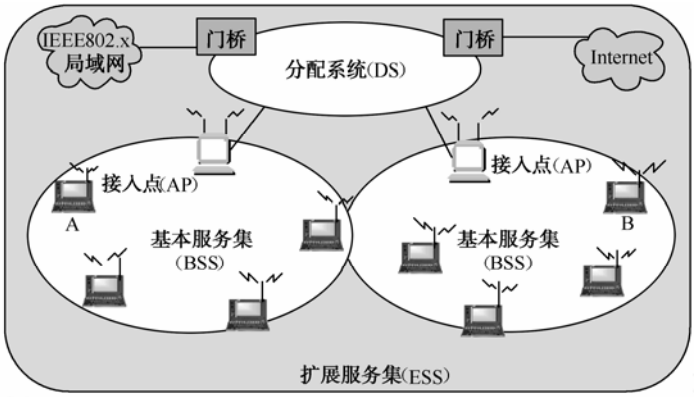


图 4.17 IEEE 802.11 的基本结构模型

一个 BSS 包括一个基站和若干个移动站，所有的站均运行同样的 MAC 协议并以争用方式共享同样的无线传输介质。基本服务集类似于无线移动通信的蜂窝小区。在 IEEE 802.11 标准中，BSS 中的基站称为接入点（Access Point，AP）。一个 BSS 可以是孤立的，也可以通过接入点 AP 连接到一个主干分配系统（Distribution System，DS），然后再接入到另一个 BSS，这样就构成了一个扩展服务集 ESS（Extended Service Set，ESS）。主干分配系统可采用常用的有线以太网或其他的无线连接。接入点的作用与网桥相似，使扩展服务集成为一个在 LLC 子层上的逻辑局域网。

连接在无线局域网中的设备通常称为站。IEEE 802.11 标准按照移动性定义了下列三种站。

（1）固定站：如台式计算机和其他有线局域网中的设备。

（2）半移动站：经常改变使用场所的站，一般在移动状态下不需要保持与网络通信。

（3）移动站：在移动过程中也需要与网络通信的站，如车载计算机等。

4.4.4 IEEE 802.11 系列标准

1．IEEE 802.11 的物理层规范

IEEE 802.11 协议定义了 WLAN 所使用的无线频段以及调制方式，并进一步分为 IEEE 802.11b、IEEE 802.11a、IEEE 802.11g 和 IEEE 802.11n 四种类型。

（1）IEEE 802.11b 使用 2.4 GHz 频带，标称传输速率为 11 Mbps，实际为 7～8 Mbps。

（2）IEEE 802.11a 使用 5 GHz 频带，传输速率为 54Mbps。

（3）IEEE 802.11g 使用 2.4G 频段，传输速率为 20Mbps 以上。

（4）IEEE802.11n 使用双频（2.4GHz 和 5GHz）工作模式。传输速率增加至 108Mbps 以上，最高速率可达 320Mbps。

2.4GHz 频带是一个容易受微波炉、无绳电话和其他无线设备干扰的频带，5GHz 频带是

一个干扰较小的频带。

IEEE 802.11 定义了下列三种物理层的实现方法。

（1）红外线（InfraRed，IR）：IR 使用波长为 850～950nm 的红外在室内传送数据。数据速率为 1Mbps 和 2Mbps。

（2）直接序列扩频（Direct Sequence Spread Spectrum，DSSS）：DSSS 运行在 2.4GHz ISM 频带上，它能够使用 7 条信道，每条信道的数据速率为 1Mbps 或 2Mbps。

（3）跳频扩频（Frequency Hopping Spread Spectrum，FHSS）：FHSS 是扩频技术中常用的一种。它运行在 2.4GHz ISM 频带上，数据速率为 1Mbps 或 2Mbps。

2．IEEE 802.11 定义的服务

IEEE 802.11 定义了无线局域网必须提供的服务，这些服务主要有下列 5 种。

（1）联系（Association）：在一个节点和一个访问点之间建立一个初始的联系。

（2）重联系（Reassociation）：把一个已经建立联系的节点从一个访问点转移到另一个访问点，从而使节点能够从一个基本服务集转移到另一个基本服务集。

（3）终止联系（Disassociation）：节点离开一个扩展访问集或关机前需要通知访问点联系终止。

（4）认证（Authentication）：认证服务用于在互相需要通信的节点之间建立起彼此识别身份的标志。

（5）隐私权（Privacy）：标准提供的加密选项用于防止信息被窃听者收到，以保护隐私权。

3．IEEE 802.11 中的MAC子层

IEEE 802.11 工作组考虑了两种介质访问控制（MAC）算法：一种是分布式访问控制，它和以太网类似，通过载波侦听方法来控制每个访问节点；另一种算法是集中式访问控制，它是由一个中心节点来协调多节点的访问控制。分布式访问控制适用于特殊网络，而集中式控制适用于几个互连的无线节点和一个与有线主干网连接的基站。

IEEE 802.11 工作组最后决定采用分布式基础无线网的介质访问控制算法。IEEE 802.11 的介质访问控制（MAC）层又分为 2 个子层：分布式协调功能子层与点协调功能子层。

分布式协调功能子层使用一种简单的CSMA 算法，没有冲突检测功能。按照简单的CSMA 的介质访问规则进行如下两项工作。

（1）如果一个节点要发送帧，它需要先侦听介质。如果介质空闲，节点可以发送帧；如果介质忙，节点就要推迟发送，继续侦听，直到介质空闲。

（2）节点延迟一个空隙时间，再次侦听介质。如果发现介质忙，则节点按照二进制指数退避算法延时，并继续侦听介质。如果介质空闲，节点就可以传输。

二进制指数退避算法提供了一种处理重负载的方法。但是，多次发送失败，将会导致越来越长的退避时间。

在分布式访问控制子层之上有一个集中式控制选项。点协调功能是通过在网中设置集中式的轮询主管“点”的方式，使用轮询方法来解决多节点争用公用信道问题，提供无竞争的服务。

4.4.5　无线局域网的组建

图 4.18 是会议中心无线局域网的拓扑结构。该会议中心使用无线局域网的解决方案来实现会议中心的网络接入。一个 AP 的最佳接入用户数量大约是 30，因此在实际应用中应根据用户数确定接入点的个数。在会议中心，通过 AP 构成两个无线局域网，各接入点与交换机连接，通过交换机与办公大楼的有线局域网相连，并可通过路由器与 Internet 连接起来。

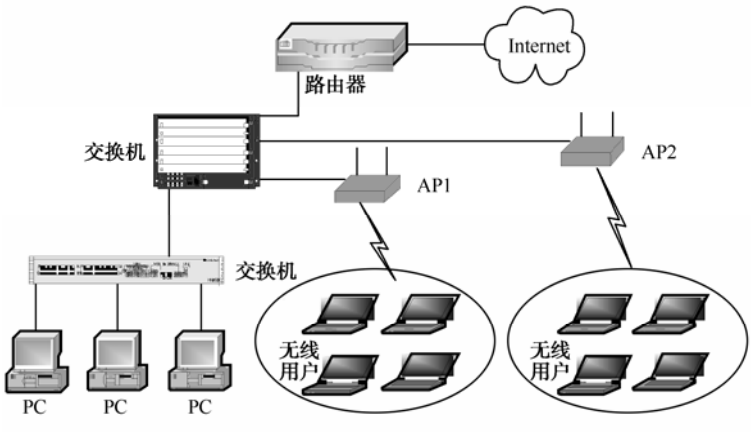


图 4.18　会议中心无线局域网络的拓扑结构

4.5　组网实例

4.5.1　学生宿舍无线局域网

一般大学的学生宿舍有 4～8 名学生，因考虑携带的方便性，不少学生更喜欢使用笔记本电脑。目前的笔记本电脑都自带无线网卡，因此在学生宿舍组建无线网络更受欢迎。

学生宿舍组建无线局域网，要看各校宿舍的布线情况。有些新建的宿舍，每个学生均设计了信息点，每层楼都设有接入层交换机，学生上网不需要再购买交换机，直接接入信息点就可以上网。大部分宿舍只设计了一个信息点，如果同一个宿舍的学生共享接入校园网，实现无线上网，可以采用交换机＋无线 AP 方式无线上网，也可采用无线路由器方式无线上网。学生宿舍无线局域网的拓扑结构如图 4.19 所示。

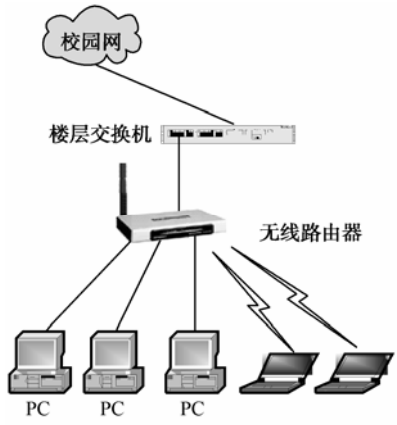


图 4.19　学生宿舍无线局域网的拓扑结构

学生宿舍选用无线路由器要注意有线端口的数量，如无线路由器有 4 个 LAN 端口的最多只能供 4 台计算机以有线方式上网，同时可供多台计算机以无线方式上网。

4.5.2 小型企业局域网

某小型企业，因为刚刚成立，现在只有几台计算机和一台服务器。组建网络可以利用一条 ADSL 线路接入 Internet，使多台计算机可以同时上网，并且还可以实现文件共享、共享打印机等。具体方案是，将计算机、服务器与一台 8～16 口交换机相连，再通过交换机与带路由功能的 ADSL MODEM 相连接。小型企业局域网的拓扑结构如图 4.20 所示。

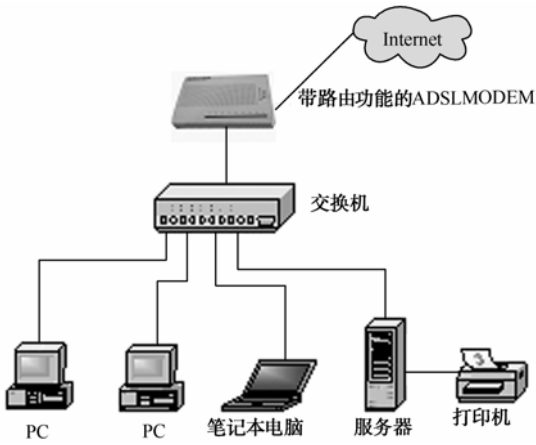


图 4.20　小型企业局域网的拓扑结构

4.5.3 中型企业局域网

一般中型商务企业需要企业网（Intranet）、企业信息系统、共享打印机、共享 Internet 接入。企业应当拥有一个稳定的网络平台，接入这个系统的设备，一般采用 100Mbps 全双工交换机、服务器和客户机。同时，需合理地划分 VLAN，可以有效地控制网络广播，减轻网络传输的负担，通过交换机的公共端口，提供不同 VLAN 之间的高效通信；通过授权对安全隔离加以控制；还要考虑接入 Internet 和远程用户接入。中型企业局域网的拓扑结构如图 4.21 所示。

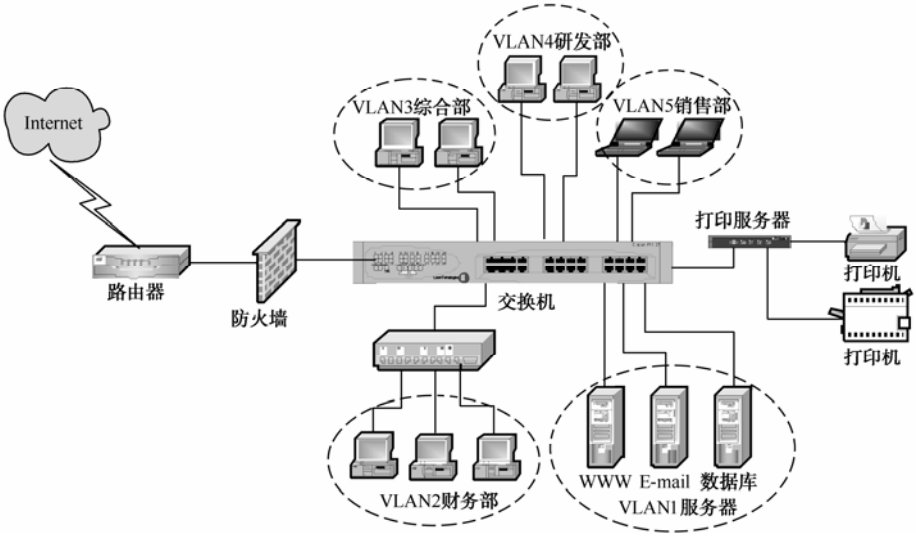


图 4.21　中型企业局域网的拓扑结构

本 章 小 结

本章介绍了局域网的主要特点、拓扑结构、传输介质和分类，讨论了 CSMA/CD 总线网、令牌环网及令牌总线网的 3 种介质访问控制技术，详细介绍了以太网的产生与发展、传统以太网、高速以太网、交换式以太网和虚拟局域网技术，最后介绍了无线局域网和组网实例。

（1）局域网具有覆盖范围小、数据传输速率高、误码率低、建网成本低、周期短、协议简单、结构灵活、便于管理和扩充等特点。

（2）局域网的特性主要涉及拓扑结构、传输介质和介质访问控制三项技术问题，其中最重要的是介质访问控制。

（3）局域网常用的拓扑结构有总线形、环形、星形三种。

（4）局域网中常用的传输介质有双绞线、同轴电缆和光纤，还有微波和红外等。

（5）常用的介质访问方法包括 CSMA/CD、令牌总线、令牌环三种。

（6）以太网的核心技术是 CSMA/CD，IEEE 802.3 标准规定了 CSMA/CD 访问方法和物理层技术规范。CSMA/CD 采用分布式控制方法，接入总线的各个节点通过竞争的方式，获得总线的使用权。只有获得使用权的节点才可以向总线发送信息帧，该信息帧被接入总线的所有节点感知。

（7）令牌传送方式是一种无冲突的介质共享方式，常用于负载较重、通信量较大的网络，地理范围也比以太网大。IEEE 802.5 是令牌环标准。

（8）IEEE 802.4 标准定义了令牌总线（Token Bus）的介质访问控制方法与相应的物理规范。从物理拓扑上看，令牌总线网为总线结构；从逻辑上看，所有主机形成一个逻辑环。

（9）以太网是应用最为广泛的局域网，包括传统以太网（10Mbps）、快速以太网（100 Mbps）、千兆以太网（1000 Mbps）和万兆以太网（10Gbps），它们都符合 IEEE 802.3 系列标准。以太网采用的传输介质有同轴电缆、双绞线、光缆等，网络速度从 10Mbps、100Mbps 到 1000Mbps，介质访问控制方法是 CSMA/CD。

（10）交换式局域网从根本上改变了共享介质工作方式，它可以通过交换机在多端口之间实现多个并发连接，实现多个节点间的并发通信，以增加带宽，改善网络性能和 QoS。

（11）VLAN 是在交换技术的基础上，通过管理软件建立起来的可跨越不同物理网段、不同网络类型的站点的逻辑工作组。

（12）WLAN 作为有线接入方式的补充，最主要的优势在于无需布线，相对于有线网络，无线局域网的组建、配置和维护较为容易。

（13）无线局域网使用的是无线传输介质，按照所采用的技术可以分为三类：红外线技术、扩频技术和窄带微波技术。

（14）目前普遍采用的无线局域网标准是 IEEE 802.11 标准，也就是俗称的 WiFi。

思 考 题

一、填空题

1．决定局域网特性的三要素是_____、_____和_____。

2．以太网使用_____介质访问控制方法，而 FDDI 则使用_____介质访问控制方法。

3．在将计算机与 10Base-T 集线器进行连接时，UTP 电缆的长度不能大于_____m。

4．以太网交换机的数据转发方式可以分为_____、_____和_____3 类。
5．交换式局域网的核心设备是_____。
6．无线局域网的实现技术有_____、_____和_____3 类。

二、单项选择题

1．MAC 地址通常存储在计算机的（　　）。
A．内存中　　B．网卡上　　C．硬盘上　　D．高速缓冲区
2．在以太网中，冲突（　　）。
A．是由于介质访问控制方法的错误使用造成的
B．是由于网络管理员的失误造成的
C．是一种正常现象
D．是一种不正常现象
3．下面关于以太网的描述中哪个是正确的？（　　）
A．数据是以广播方式发送的
B．所有节点可以同时发送和接收数据
C．两个节点相互通信时，第三个节点不检测总线上的信号
D．网络中有一个控制中心，用于控制所有节点的发送和接收
4．下列哪种说法是正确的？（　　）
A．集线器可以对接收到的信号进行放大
B．集线器具有信息过滤功能
C．集线器具有路径检测功能
D．集线器具有交换功能
5．以太网交换机中的端口/MAC 地址映射表（　　）。
A．是由交换机的生产厂商建立的
B．是交换机在数据转发过程中通过学习动态建立的
C．是由网络管理员建立的
D．是由网络用户利用特殊的命令建立的
6．下列哪种说法是错误的？（　　）
A．以太网交换机可以对通过的信息进行过滤
B．以太网交换机中端口的速率可能不同
C．在交换式以太网中可以划分 VLAN
D．利用多个以太网交换机组成的局域网不能出现环
7．虚拟局域网的技术基础是（　　）技术。
A．局域网交换　　B．双绞线　　C．冲突检测　　D．光纤

三、问答题

1．局域网有哪些特点？它是如何进行分类的？局域网中有哪几种拓扑结构？
2．常用的介质访问控制方法有哪些？它们被定义为 IEEE 的哪些标准？
3．简述 CSMA/CD 的原理和过程。
4．10Base-2、100Base-T 分别代表什么含义？
5．什么是 MAC 地址？MAC 地址是如何表示的？
6．快速以太网有哪几种组网方式？各有什么特点？

7．与传统 LAN 相比，交换式 LAN 有哪些优点？

8．什么是 VLAN？它有什么特点？

9．无线局域网的主要应用领域有哪些？最基本的无线上网设备有哪几种？

实训 4　小型企业局域网的组建

一、实训目的

1．了解网络组建的实际过程。

2．熟悉局域网的安装步骤。

3．掌握网络系统的调试。

二、实训环境

某公司拥有 10 台计算机，需要连网，实现网络办公。

三、实训要求

（1）使用双绞线实现物理连接。

（2）各计算机实现 100Mbps 到桌面。

四、实训步骤

1．各计算机要求实现 100Mbps 到桌面，也就是每台计算机都要独享 100Mbps 带宽，所以，网络设备选择 16 口 10Mbps/100Mbps 自适应交换机，选用 10Mbps/100Mbps 自适应网卡。

2．为每台计算机安装网卡。

（1）确保有以下工具：一把十字形螺丝刀、一根接地的导线和一个接地的小垫子以防止内部元器件静电放电。同时，还要有足够的工作空间来操作。

（2）切断计算机的电源。

（3）打开机箱。机箱有几种不同的固定方式，对于最新式的计算机，用四枚或六枚十字形螺钉把挡板固定在后面板上，也可以采用其他方式。卸下所有必须卸掉的螺钉，移开机箱。

（4）由于 10Mbps/100Mbps 自适应网络都为 PCI 总线，所以应将网络接口卡安装在计算机的主板上的 PCI 插槽。选择一个插槽安装网络接口卡，并移掉计算机后面板上该插槽的金属挡板。

（5）把网络接口卡竖起，使其插接头与插槽垂直对应，插入插槽，用力按下网络接口卡使其与插槽结合牢固。如果插入正确，即使左右摇晃，它也不会松动。如果插得不牢固，有可能造成连接问题。

（6）网络接口卡边缘处的金属托架应该固定在先前插槽的金属挡板的位置。用一枚十字形螺钉固定好网络接口卡。

（7）检查是否弄松了计算机内的其他线缆或板卡，是否把螺钉或金属碎片遗留在计算机内。

（8）重新盖上机箱盖，并把在第（3）步中取下的螺钉拧上。

3．安装网卡驱动程序。

（1）重新启动计算机。

（2）只要你未禁止即插即用功能，Windows 2000 就会自动检测到新硬件。一旦检测出网络接口卡，系统就会提示你选择正确的驱动程序。

（3）选择“搜索适用于我的设备的驱动程序（推荐）”，单击“下一步”按钮。

（4）选择“指定位置”，单击“下一步”按钮。

（5）指定驱动程序文件所在位置，如 F：\DRIVERS。

（6）如系统找到驱动程序，系统会提示所找到驱动程序文件名及位置。单击“下一步”按钮。

（7）系统自动安装驱动程序，单击“完成”按钮。

4．根据地理分布图，可知交换机的最佳放置位置，因为计算机到达该位置的距离最短。

根据每台计算机达到交换机的实际距离制作双绞线。注意该距离并非直线距离，因为布线时应使线缆尽量隐蔽，应绕墙连接。

5．双绞线制作：按照 EIA568B 标准制作直通线，将计算机与交换机相连。

6．实现软件（逻辑）连接。

为 Windows 2000 计算机添加协议，其他操作系统的添加协议方法与其大致相同。同种协议在计算机间可以通信。在系统上安装 TCP/IP 协议。

（1）右击“网上邻居”，单击“属性”。

（2）右击“本地连接”单击“属性”。

（3）在“本地连接属性”框中，选择“TCP/IP 协议”，单击“属性”。

（4）在“Internet 协议（TCP/IP）属性”框中，选择“使用下面的 IP 地址”项。在输入框中输入 IP 地址和子网掩码，如将计算机 IP 设置 192.168.0.1 至 192.168.0.10 区段。

（5）利用 Ping 命令检测网络连通情况。

第 5 章　Windows网络服务器的配置与管理

本章要点

Windows 是当今在个人计算机上应用最广泛的网络操作系统。本章将讲述 Windows 网络服务器的权限管理、活动目录及用户管理的一些基本概念，介绍 Windows 网络服务器的常用服务程序的配置方法。

本章目标

- 了解 Windows 网络操作系统和网络服务的基本特性
- 掌握 Windows 用户和组的配置方法
- 熟悉常用网络服务的功能及常见网络服务器的配置方法

5.1　概述

服务器这个概念比较容易混淆，通常有两方面的含义：服务设备（即通常意义上的“服务器”）和服务软件。

服务设备通常是指那些具有较高计算能力、能够提供给多个用户使用的硬件（计算机），一般称为服务器。服务器与 PC 不同，PC 通常只为一个用户服务。服务器与主机不同，主机是通过提供终端给用户使用的，服务器是通过网络提供给客户端用户使用的。

服务软件指的是那些提供服务功能的软件，这类软件一般运行于服务器（硬件）中，一般称为“服务”。服务软件以客户端-服务器或浏览器-服务器的方式工作。它们通常随操作系统的启动而启动，直到系统关闭或服务器管理员中止其运行才会停下来，客户端软件或浏览器是通过网络协议调用其功能以及与其交换数据的。

本章所指的服务器的配置与管理实质上指的是配置与管理在服务器（硬件）上运行的服务（软件）。本章介绍了 Windows 网络系统本身的一些基本配置工作，如用户和组账号、NTFS 权限配置等。

5.2　用户组和账号

Windows 的每个用户都必须有一个系统账号，以便利用这个账号登录到域，然后访问网络上的资源，或者利用这个账号登录到某台计算机，然后访问该计算机的资源。

在 Windows 网络中有两种主要的账号类型：域用户账号和本地用户账号。

（1）域用户账号：存储在域控制器的活动目录数据库中。用户可以利用域用户账号登录域，并利用它访问网络上的资源，例如，访问域中其他计算机内的文件、打印机等资源。

（2）本地用户账号：存储在非域控制器的“本地安全账户数据库”（Windows 的系统数据库）中。用户可以利用本地用户账号在该账户所在的计算机上登录，但是这个账号只能访问这台计算机内的资源，无法直接访问网络上其他计算机的资源。如果要访问其他计算机的资

源，则必须输入被访问计算机的账号和密码。

5.2.1 管理本地用户和组

“本地用户和组”位于“计算机管理”中，用户可以利用这一组管理工具来管理单台本地或远程计算机。可以使用“本地用户和组”保护并管理存储在本地计算机上的用户账户和组。可以在特定计算机和仅这台计算机上分配本地用户或组账户的权限和权力。可以在以下客户端和服务器操作系统上使用“本地用户和组”：

（1）运行 Windows 2000 及以上的 Professional 版本的客户端计算机。

（2）运行 Windows 2000 及以上的 Server 版本的成员服务器。

（3）运行 Windows 2000 及以上的 Server 版本的独立服务器。

通过“本地用户和组”，可以为用户和组分配权力和权限，从而限制用户和组执行某些操作的能力。权力可授权用户在计算机上执行某些操作，如备份文件和文件夹或者关机。权限是与对象（通常是文件、文件夹或打印机）相关联的一种规则，它规定哪些用户可以访问该对象以及以何种方式访问。

成员服务器提升为域控制器后，就无法使用“本地用户和组”查看本地用户和组账户。不过，可以使用域控制器上的“本地用户和组”控制网络上的远程计算机（不是域控制器）。可使用“Active Directory 用户和计算机”管理 Active Directory 中的用户和组。

1．管理本地用户

1）创建本地用户账户

（1）打开“计算机管理”窗口。

（2）在控制台树中，右击“用户”

（3）单击“操作”菜单中的“新用户”。

（4）在如图 5.1 所示的对话框中键入适当的信息，选中或清除以下复选框：

① 用户下次登录时须更改密码。

② 用户不能更改密码。

③ 密码永不过期。

④ 账户已禁用。

（5）单击“创建”按钮，然后单击“关闭”按钮。

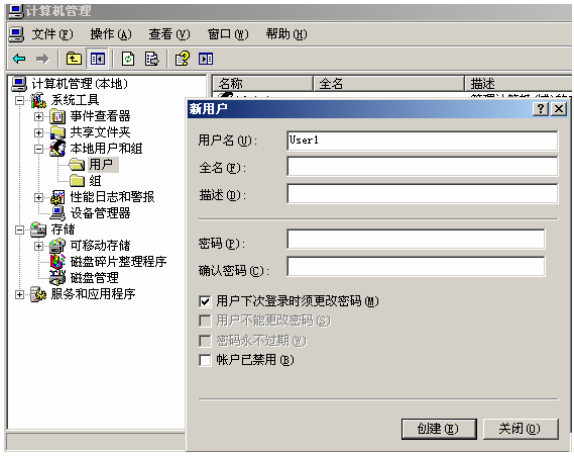


图 5.1 “新用户”对话框

2）重置本地用户账户的密码

（1）打开“计算机管理”窗口。

（2）在控制台树中，单击“用户”。

（3）右键单击要为其重置密码的用户账户，然后单击“设置密码”。

（4）阅读警告消息，如果要继续，单击“继续”按钮。

（5）在如图 5.2 所示的对话框的“新密码”和“确认密码”框中，键入新密码，然后单击“确定”按钮。

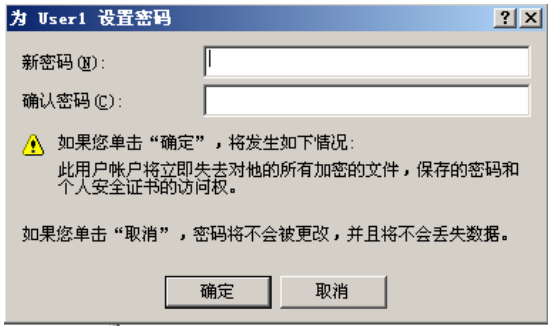


图 5.2　重置本地用户账户的密码

3）禁用或激活本地用户账户

（1）打开“计算机管理”窗口。

（2）在控制台树中，单击“用户”。

（3）右键单击要更改的用户账户，然后单击“属性”。

（4）在如图 5.3 所示的对话框中，执行以下任一操作：

① 若禁用所选的用户账户，则选中“账户已禁用”复选框。

② 若激活所选的用户账户，则清除“账户已禁用”复选框。

图 5.3　禁用或激活本地用户账户

4）重命名本地用户

（1）打开“计算机管理”窗口。

（2）在控制台树中，单击“用户”，如图 5.4 所示。

（3）右键单击要重命名的用户账户，然后单击“重命名”。键入新的用户名，然后按 Enter 键。

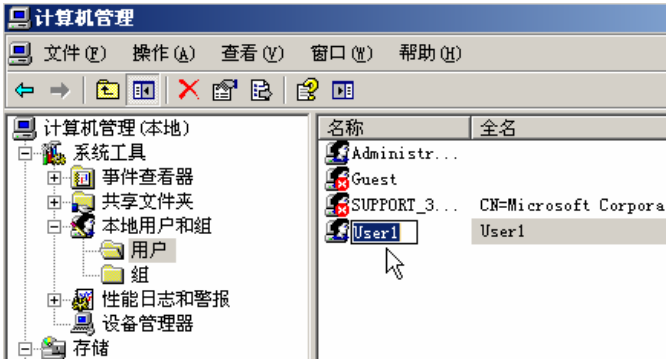


图 5.4　重命名本地用户

5）指派本地用户账户的主文件夹

（1）打开“计算机管理”窗口。

（2）在控制台树中，单击“用户”。

（3）右键单击要为其指定主文件夹的用户账户，然后单击“属性”。

（4）在如图 5.5 所示的对话框的“配置文件”选项卡中，执行下列某项操作：

① 若指定本地主文件夹，则选中“本地路径”单选钮，然后键入路径，如 c:\users\nicolette

② 若在共享资源上指定主文件夹，则选中“连接”单选钮，然后单击合适的驱动器盘符，并键入网络路径，如\\airedale\users\nathan。

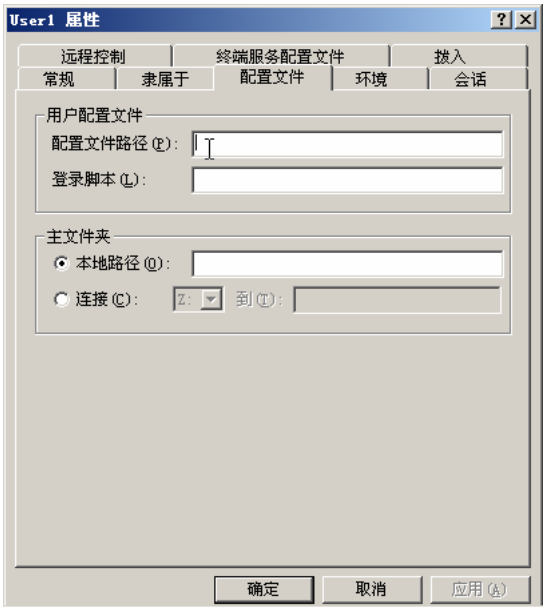


图 5.5　指派本地用户账户的主文件夹

2．管理本地组

1）创建本地组

（1）打开“计算机管理”窗口。

（2）单击控制台树中的“组”。

（3）单击“操作”菜单的“新建组”。

（4）在如图 5.6 所示的对话框的“组名”框中，键入新组的名称。

（5）在“描述”框中，键入新组的说明。

（6）若向新组添加一个或多个成员，则单击“添加”按钮。

（7）在“选择用户”对话框中，执行以下操作：

① 若向该组添加用户或组账户，则在“输入对象名称来选择（示例）”框中，键入要添加的用户账户或组账户的名称，然后单击“确定”按钮。

② 若向该组添加计算机账户，则单击“对象类型”按钮，选中“计算机”复选框，然后单击“确定”按钮。在“输入对象名称来选择（示例）”框中，键入要添加的计算机账户的名称，然后单击“确定”按钮。

在“新建组”对话框中，依次单击“创建”和“关闭”按钮。

图 5.6　创建本地组

2）为本地组添加成员

（1）打开“计算机管理”窗口。

（2）在控制台树中，单击“组”。

（3）右键单击要在其中添加成员的组，然后依次单击“添加到组”和“添加”。

（4）在如图 5.7 所示的“选择用户”对话框中，执行以下操作：

① 若向该组添加用户账户或组账户，则请在“输入对象名称来选择（示例）”框中，键入要添加到组的用户账户或组账户的名称，然后单击“确定”按钮。

② 若向该组添加计算机账户，则单击“对象类型”按钮，选中“计算机”复选框，然后单击“确定”按钮。在“输入对象名称来选择（示例）”框中，键入要添加到组的计算机账户的名称，然后单击“确定”按钮。

图 5.7　为本地组添加成员

3）删除本地组

（1）打开“计算机管理”按钮。

（2）单击控制台树中的“组”。

（3）右键单击要删除的组，然后单击“删除”按钮。

注意：

① 无法删除以下默认组：Administrators、Backup Operators、Guests、Network Configuration Operators、Performance Log Users、Performance Monitor Users、Power Users、Print Operators、Remote Desktop Users、Replicator、Users。

② 不能恢复已删除的组。

③ 删除本地组只是删除这个组，而不删除该组中的用户账户、计算机账户或组账户。

④ 如果删除组，然后用相同的组名创建其他组，则必须为新组设置新的权限。它不能继承分配给原组的权限。

5.2.2　管理域用户

1．管理用户

1）新建域用户账户

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，右键单击要在其中添加域用户账户的文件夹。

（3）单击“新建”，然后单击“用户”。

（4）在如图 5.8 所示的对话框的“名”文本框中键入用户的名字。

（5）在“英文缩写”框中键入用户姓名的大写首字母。

（6）在“姓”框中键入用户的姓氏。

（7）在“姓名”框中修改、添加姓名大写首字母或姓氏与名字。

（8）在“用户登录名”框中，键入用户登录名称，单击下拉列表中的 UPN 后缀，然后单击“下一步”按钮。

（9）如果用户使用其他名称登录到运行 Windows 95、Windows 98、Windows NT 的计算机，则应将显示在“用户登录名（Windows 2000 以前版本）”框中的用户登录名改成其他名称。

（10）在“密码”和“确认密码”框中，键入用户的密码，然后选择适当的密码选项。

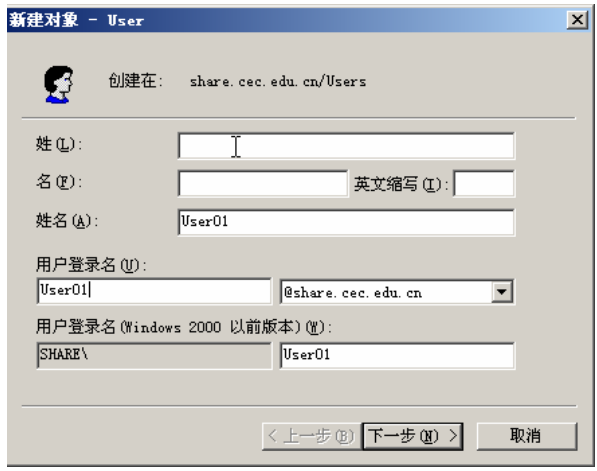


图 5.8　新建域用户账户

2）重设域用户密码

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击“Users”或单击包含该用户账户的文件夹。

（3）在详细信息窗格中，右键单击要重设其密码的用户，然后单击“重设密码”按钮。

（4）键入并确认密码。

（5）如果想让用户在下次登录时更改该密码，则应选中“用户下次登录时须更改密码”复选框，如图 5.9 所示。

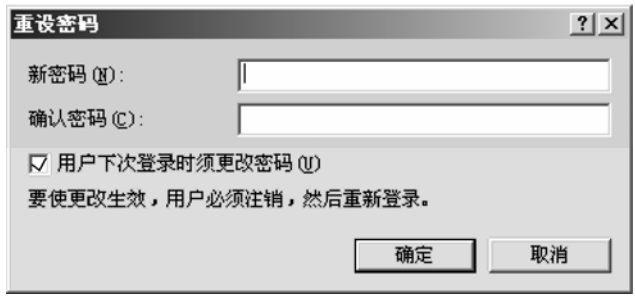


图 5.9　重设域用户密码

3）复制域用户账户

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击“Users”或单击包含该用户账户的文件夹。

（3）在详细信息窗格中，右键单击要复制的用户账户，然后单击“复制”按钮。

（4）在“名”文本框中键入用户的名字。

（5）在“姓”文本框中键入用户的姓氏。

（6）在“姓名”框中修改、添加中间名或反序的名字和姓氏。

（7）在“用户登录名”框中，键入用户登录名称，单击下拉列表中的 UPN 后缀，然后单击“下一步”按钮。

（8）如果用户使用不同的名称从运行 Windows 98、Windows 95、Windows NT 的计算机登录，则将显示在“用户登录名（Windows 2000 以前版本）”框中的用户登录名改成其他名称。

（9）在“密码”和“确认密码”框中，键入用户的密码，然后选择适当的密码选项。

（10）如果从中复制新用户账户的用户账户被禁用，则在如图 5.10 所示的对话框中单击“账户已禁用”复选框以启用新的账户。

图 5.10　复制域账户

4）*移动域用户账户*

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击“Users”或单击包含该用户账户的文件夹。

（3）在详细信息窗格中，右键单击要移动的用户，然后单击“移动”。

（4）在如图 5.11 所示的“移动”对话框中，单击用户账户要移至的文件夹。

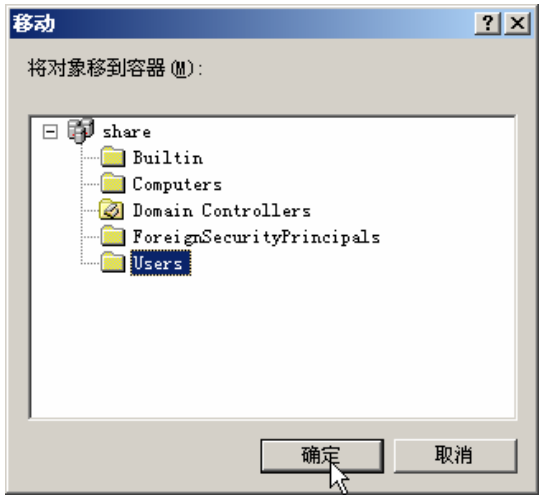


图 5.11　移动域用户账户

5）*设置登录时间*

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击“Users”或者单击包含该用户账户的文件夹。

（3）右键单击该用户账户，然后单击“属性”。

（4）在“账户”选项卡中，单击“登录时间”按钮，然后为该用户设置允许或拒绝的登

录时间，如图 5.12 所示。

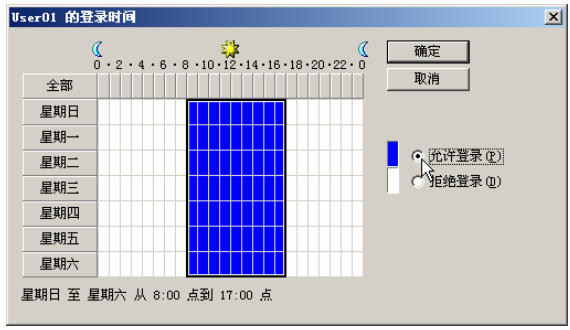


图 5.12　设置域用户的登录时间

6）禁用或启用用户账号

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击“用户”或单击包含该用户账户的文件夹。

（3）在详细信息窗格中，右键单击该用户。

（4）根据账户的状态，执行下列操作之一：

① 要禁用，请单击“禁用账户”。

② 要启用，请单击“启用账户”。

7）更改用户的主要组

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击“Users”或单击包含该用户账户的文件夹。

（3）在详细信息窗格中，右键单击要更改的用户，然后单击“属性”。

（4）在如图 5.13 所示的对话框的“隶属于”选项卡中，单击要设置为用户主要组的组，然后单击“设置主要组”按钮。

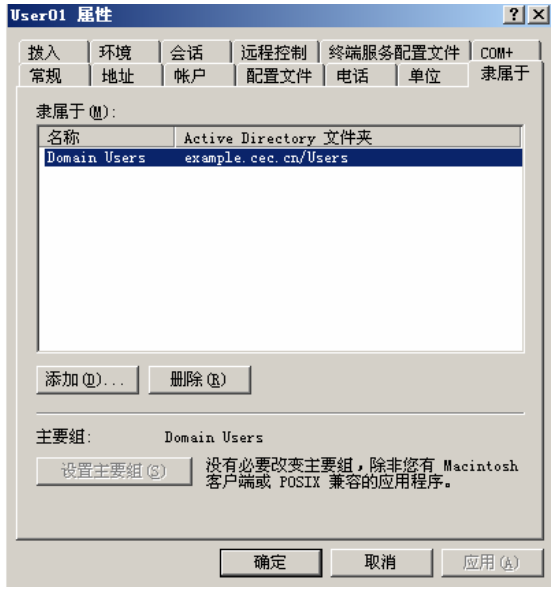


图 5.13　更改用户的主要组

8）删除域用户

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击“Users”或单击包含该用户账户的文件夹。

（3）在详细信息窗格中，右键单击该用户账户，然后单击“删除”按钮。

2．管理用户组

1）创建新组

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，右键单击要在其中添加新组的文件夹。

（3）单击“新建”，然后单击“组”。

（4）键入新组的名称。

（5）在如图 5.14 所示的对话框的“组作用域”区中，单击某个选项。

（6）在“组类型”区中，单击某个选项。

图 5.14　创建域用户组

2）为域用户组添加成员

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击某个文件夹，该文件夹包含要在其中添加成员的组。

（3）右键单击详细信息窗格中的组，然后单击“属性”。

（4）在“成员”选项卡中，单击“添加”按钮。

（5）在“输入对象名称来选择（示例）”框中，键入要添加到组的用户、组或计算机的名称，然后单击“确定”按钮，如图 5.15 所示。

3）将组转换为另一种组类型

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击包含要转换为另一种组类型的组的文件夹。

（3）右键单击详细信息窗格中的组，然后单击“属性”。

（4）在如图 5.16 所示的对话框的“常规”选项卡的“组类型”区中，单击组类型。

注意：若要转换组，必须将域功能级别设置为 Windows 2000 本机或更高版本。当将域功能级别设置为 Windows 2000 混合模式时，不能转换组。

图 5.15　为域用户组添加成员

4）更改组作用域

（1）打开 “Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击某个文件夹，该文件夹包含要更改其组作用域的组。

（3）右键单击详细信息窗格中的组，然后单击“属性”。

（4）在如图 5.17 所示的对话框的“常规”选项卡的“组作用域”区中，单击组作用域。

注意：只能在域功能级别设置为 Windows 2000 本机或更高级别时，更改组作用域。

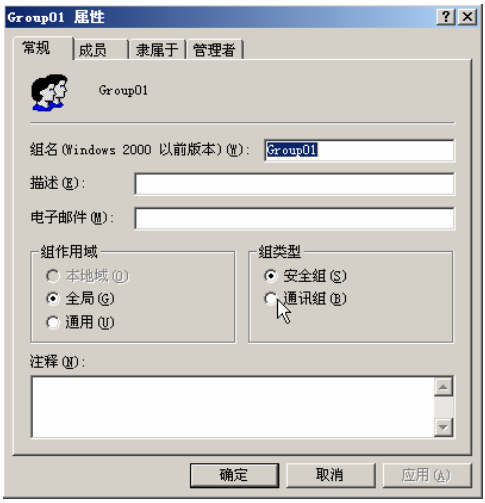


图 5.16　转换组类型

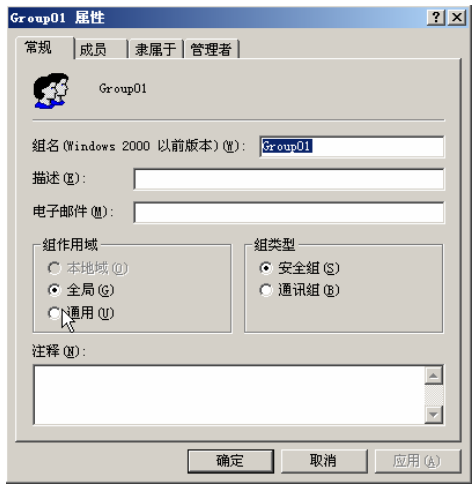


图 5.17　更改组作用域

5）删除组

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击包含要删除组的文件夹。

（3）在详细信息窗格中，右键单击该组，然后单击“删除”按钮。

6）查找包含某个用户的组

（1）打开“Active Directory 用户和计算机”窗口。

（2）在控制台树中，单击“Users”或单击包含该用户账户的文件夹。

（3）在详细信息窗格中，右键单击用户账户，然后单击“属性”。

（4）单击“隶属于”选项卡。

7）将用户权限指派到 Active Directory 中的组

（1）打开“默认域控制器安全设置”窗口。

（2）在控制台树中，单击“用户权限分配”。

（3）在详细信息窗格中，双击要指派的用户权限。

（4）如果此按钮显示无效，则选中如图 5.18 所示的对话框的“定义这些策略设置”复选框。

（5）键入要为其指派此权限的组的名称。

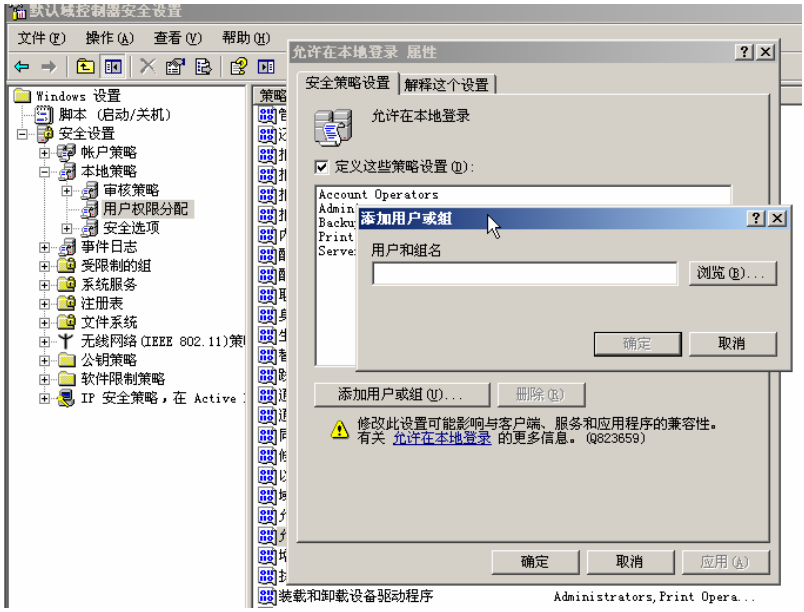


图 5.18　将用户权限指派到 Active Directory 中的组

5.2.3　内置组

Windows Server 2003 的内置组有以下两类。

1．普通内置组

（1）Administrators ：属于该 Administrators 本地组内的用户，都具备系统管理员的权限，它们拥有对这台计算机最大的控制权限，可以执行整台计算机的管理任务。内置的系统管理员 Administrator 就是本地组的成员，而且无法将它从该组删除。

如果这台计算机已加入域，则域的 Domain Admins 会自动地加入到该计算机的 Administrators 组内。也就是说，域上的系统管理员在这台计算机上也具备系统管理员的权限。

（2）Backup Operators：在该组内的成员，不论它们是否有权访问这台计算机中的文件夹或文件，都可以通过“开始”→“所有程序”→“附件”→“系统工具”→“备份”的途径，备份与还原这些文件夹与文件。

（3）Guests：供没有用户账户但需要访问本地计算机内资源的用户使用。该组的成员无

法永久地改变其桌面的工作环境。该组最常见的默认成员为用户账户 Guest。

（4）Network Configuration Operators：该组内的用户可以在客户端执行一般的网络设置任务，例如更改 IP 地址，但是不可以安装/删除驱动程序与服务，也不可以执行与网络服务器设置有关的任务，例如 DNS 服务器、DHCP 服务器的设置。

（5）Power Users：该组内的用户具有比 Users 组更多的权力，但是比 Administrators 组拥有的权力少一些，例如可以：

① 创建、删除、更改本地用户账户。

② 创建、删除、管理本地计算机内的共享文件夹与共享打印机。

③ 自定义系统设置，例如更改计算机时间、关闭计算机等。

（6）Power Users：该组的成员不可以更改 Administrators 与 Backup Operators、无法夺取文件的所有权、无法备份与还原文件、无法安装删除与删除设备驱动程序、无法管理安全与审核日志。

（7）Remote Desktop Users：该组的成员可以通过远程计算机登录，例如，利用终端服务器从远程计算机登录。

（8）Users：该组员只拥有一些基本的权力，例如运行应用程序，但是他们不能修改操作系统的设置、不能更改其他用户的数据、不能关闭服务器级的计算机。

所有添加的本地用户账户者自动属于该组。

如果这台计算机已经加入域，则域的 Domain Users 会自动地被加入该计算机的 Users 组中。

2．内置特殊组

（1）Everyone：任何一个用户都属于这个组。注意，如果 Guest 账户被启用时，则给 Everyone 这个组指派权限时必须小心，因为当一个没有账户的用户连接计算机时，他被允许自动利用 Guest 账户连接，但是因为 Guest 也属于 Everyone 组，所以他将具备 Everyone 所拥有的权限。

（2）Authenticated Users：任何一个利用有效的用户账户连接的用户都属于这个组。建议在设置权限时，尽量针对 Authenticated Users 组进行设置，而不要针对 Everyone 进行设置。

（3）Interactive：任何在本地登录的用户都属于这个组。

（4）Network：任何通过网络连接此计算机的用户都属于这个组。

（5）Creator Owner：文件夹、文件或打印文件等资源的创建者，就是该资源的 Creator Owner（创建所有者）。不过，如果创建者是属于 Administrators 组内的成员，则其 Creator Owner 为 Administrators 组。

（6）Anonymous Logon：任何未利用有效的 Windows Server 2003 账户连接的用户，都属于这个组。注意，在 Windows 2003 内，Everyone 组内并不包含“Anonymous Logon”组。

5.3 NTFS权限与活动目录

5.3.1 NTFS权限概述

NTFS 是 Windows NT 以及之后的 Windows 2000、Windows XP、Windows Server 2003、Windows Server 2008、Windows Vista 和 Windows 7 的标准文件系统。

NTFS 取代了文件分配表（FAT）文件系统，为 Microsoft 的 Windows 系列操作系统提供

文件系统。NTFS 对 FAT 和 HPFS（高性能文件系统）做了若干改进，例如，支持元数据，并且使用了高级数据结构，以便于改善性能、可靠性和磁盘空间利用率，并提供了若干附加扩展功能，如访问控制列表（ACL）和文件系统日志。该文件系统的详细定义属于商业秘密，Microsoft 已经将其注册为知识产权产品。

在 Windows 的早期版本（Windows 3.x/9x/Me）及 DOS（Disk Operate System）操作系统中，只要知道了账户和密码，就可以实现对计算机完全控制（在 DOS 中不需要账号和密码，谁使用计算机，谁就能完全控制该计算机），在这种情况下是无法实现针对某个账户只允许读取某个文件夹或者某个文件的控制功能。有了 NTFS 以后，就可以在操作系统中实现文件夹及文件级别的安全控制。

如果要使用 NTFS 的权限管理功能，要求被管理的磁盘分区必须是 NTFS 格式的。可以将新磁盘分区格式化为 NTFS 格式，也可以通过 Convert 命令将 FAT、FAT16、FAT32 转换为 NTFS 系统，命令格式如下：

convert x: /fs:ntfs

其中的 x 可以用实际的盘符替换。

值得注意的是，Windows NT 以前版本的 Windows 无法识别 NTFS 格式的分区，即在 Windows 98 等早期的操作系统中无法识别使用 NTFS 格式的分区，而且该命令是不可逆的，也就是说该命令只能将 FAT32 转换成 NTFS 格式，而无法将 NTFS 格式转换成 FAT32 格式。如果要转换，则用 PQ 等软件才能实现。

5.3.2 NTFS权限设置

在以 NT 内核为基础的 Windows 中，权限主要分为七大类：完全控制、修改、读取和运行、列出文件夹目录、读取、写入、特别的权限。NTFS 的权限及其含义如表 5.1 所示。NTFS 权限的等级高低如下：

完全控制 > 特别的权限 > 列出文件夹目录 > 读取和运行 > 修改> 写入 >读取

表 5.1 NTFS 的权限及其含义

NTFS 权限	含 义
完全控制	对指定文件或目录拥有不受限制的完全访问。选中了“完全控制”，下面的第 2 项～第 5 项属性将被自动选中
修改	选中了“修改”，下面的四项属性将被自动选中。下面的任何一项没有被选中时，“修改”条件将不再成立
读取和运行	允许读取和运行指定文件或在指定目录下的任何文件，“列出文件夹目录”和“读取”是“读取和运行”的必要条件
列出文件夹目录	这个权限只针对目录有效，如果选择该权限，则只能浏览该卷或目录下的子目录列表，不能读取、运行或修改其下的文件
读取	能够读取指定文件或目录下的数据
写入	能在指定文件或目录下写入数据
特别的权限	对以上的六种权限进行了细分

设置步骤：

（1）选择 NTFS 分区中的一个文件或文件夹，在其快捷菜单中选择“属性”。

（2）在弹出的如图 5.19 所示的“属性”对话框中选择“安全”选项卡。

（3）单击“添加”按钮，在弹出的对话框中，选中指定用户，单击“添加”按钮，单击“确定”按钮。

（4）单击刚才选中的用户，在指定权限后面的“允许”方框中单击选中。

（5）改用刚才选中的用户登录系统，再尝试对已经设置权限的文件夹进行操作，查看有什么不同。

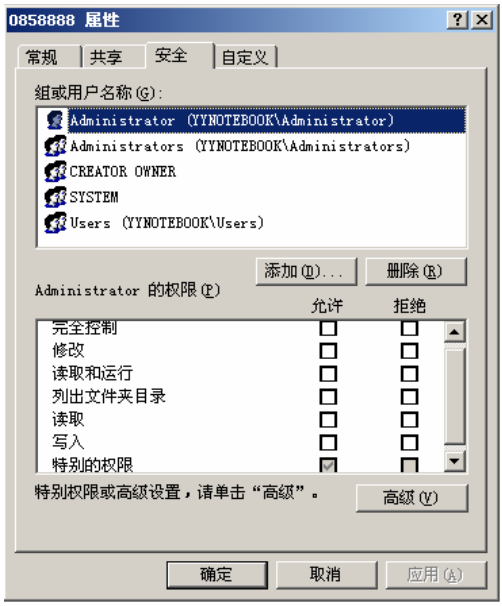


图 5.19　用户权限设置

5.4　DNS的配置

5.4.1　DNS的基本概念

DNS（Domain Name System）或者 Domain Name Service，称为域名系统或者域名服务。DNS 为 Internet 上的主机分配域名地址和 IP 地址。浏览者访问网站的域名地址，DNS 就会自动把域名地址转为 IP 地址。这就像我们日常生活的 114 的电话查询系统：当你不知道某个公司的电话时，你就拨通 114，告诉 114 你要查询的公司名称，如果该公司登记了号码，114 就会告诉你该公司的电话号码。DNS 也起着类似的作用：你不知道 IP 地址，用域名通过 DNS 查询，只要该域名已经注册，就能查到相应的 IP 地址。

因此，注册服务商除了帮你注册域名外，一般都会同时提供 DNS 服务（将域名解析到你指定的 IP 地址）。域名和 DNS 服务两者缺一不可。

以下是域名和域名服务的一些基本概念：

（1）域名解析是通过域名服务器进行的，它的任务就是把域名解析为对应的 IP 地址，如 A 记录、MX 记录等。

（2）任何域名都至少有一个 DNS，一般是 2 个。因为 DNS 可以轮回处理，若第一个 DNS

解析失败则可以使用第二个 DNS；只要有一个 DNS 解析正常，就不会影响域名的正常使用。

（3）A（Address）记录是用来指定主机名（或域名）对应的 IP 地址记录。用户可以将该域名下的网站服务器指向到自己网站空间主机的 IP 地址上。同时，也可以设置域名的二级域名。

（4）MX 记录，即邮件路由记录，用户可以将该域名下的邮件服务器指向到自己的网站空间主机的 IP 地址上，然后即可自行操控所有的邮箱设置。用户只需在线将该域名对应的 IP 地址填写成自己邮件服务器的 IP 地址，即可将该域名下的邮件全部转到自己设定相应的邮件服务器上。

5.4.2 配置DNS

下面以 Windows Server 2003 为例，为其域名系统 （DNS） 配置 Internet 访问。

1．配置前的准备工作

（1）DNS 的服务器不应该使用动态分配的 IP 地址，因为地址的动态更改会使客户端与 DNS 服务器失去联系。应首先保证为该服务器分配一个静态 Internet 协议（IP）地址。

（2）在“高级 TCP/IP 设置”对话框中选中“DNS”选项卡。附加主要的和连接特定的 DNS 后缀，并选中“附加主 DNS 后缀的父后缀”复选框和“在 DNS 中注册此连接的地址”复选框，如图 5.20 所示。

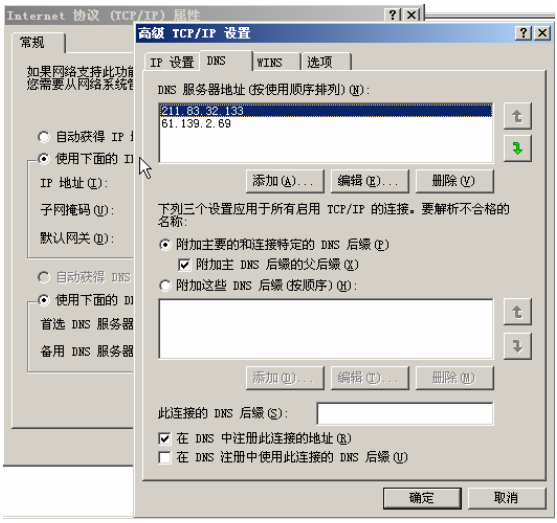


图 5.20 “高级 TCP/IP 设置”对话框

注意，运行 Windows Server 2003 的 DNS 服务器必须将其 DNS 服务器指定为它本身。

如果该服务器需要解析来自它的 Internet 服务提供商 （ISP） 的名称，还必须配置一台转发器。

（3）确保系统中已经安装了 DNS 服务，并保证该服务能正常运行，如图 5.21 所示。

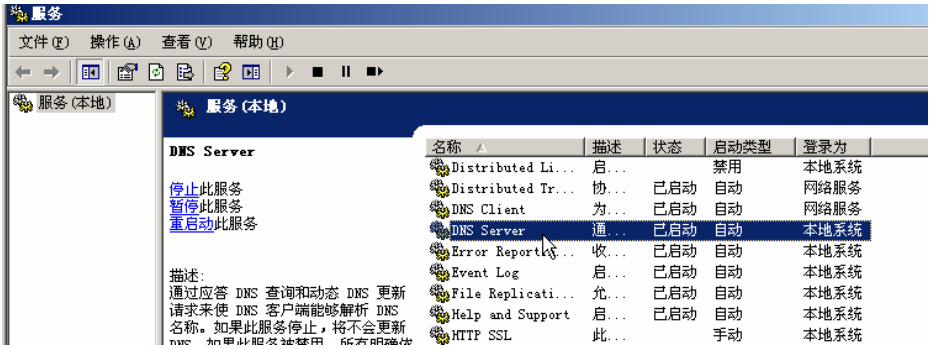


图 5.21　DNS 服务

2．配置 DNS 服务器

打开 Microsoft 管理控制台（MMC）中的 DNS 管理单元配置 DNS。

（1）右击正向搜索区域，然后单击新建区域。

（2）当“新建区域向导”启动后，单击“下一步”按钮。

（3）选择区域类型。区域类型包括下列三类。

① 主要区域：创建可以直接在此服务器上更新的区域的副本。此区域信息存储在一个.dns 文本文件中。

② 辅助区域：标准辅助区域从它的主 DNS 服务器复制所有信息。主 DNS 服务器可以是为区域复制而配置的 Active Directory 区域、主要区域或辅助区域。注意，我们无法修改辅助 DNS 服务器上的区域数据。所有数据都是从主 DNS 服务器复制而来。

③ 存根区域：存根区域只包含标志该区域的权威 DNS 服务器所需的资源记录。这些资源记录包括名称服务器（NS）、起始授权机构（SOA）和可能的 glue 主机（A）记录。

Active Directory 中还有一个用来存储区域的选项。此选项仅在 DNS 服务器是域控制器时可用。

新的正向搜索区域必须是主要区域或 Active Directory 集成的区域，以便它能够接受动态更新。单击“主要”按钮，然后单击“下一步”按钮。

新区域包含该基于 Active Directory 的域的定位器记录。区域名称必须与基于 Active Directory 的域的名称相同，或者是该名称的逻辑 DNS 容器。例如，如果基于 Active Directory 的域的名称为“support.microsoft.com”，那么有效的区域名称只能是“support.microsoft.com”。

（4）接受新区域文件的默认名称，单击“下一步”按钮。

3．移除根DNS 区域

运行 Windows Server 2003 的 DNS 服务器在它的名称解析过程中遵循特定的步骤。DNS 服务器首先查询它的高速缓存，然后检查它的区域记录，并将请求发送到转发器，最后使用根服务器尝试解析。

默认情况下，Microsoft DNS 服务器连接到 Internet 以便用根提示进一步处理 DNS 请求。当使用 Dcpromo 工具将服务器提升为域控制器时，域控制器需要 DNS。如果在提升过程中安装 DNS，会创建一个根区域。这个根区域向用户的 DNS 服务器表明它是一个根 Internet 服务器。因此，用户的 DNS 服务器在名称解析过程中并不使用转发器或根提示。

（1）单击“开始”，指向“管理工具”，然后单击“DNS”。

（2）展开 ServerName，其中 ServerName 是服务器的名称，单击“属性”，然后展开正

向搜索区域。

（3）右击“.”区域，然后单击“删除”按钮。

4．配置转发器

Windows Server 2003 可以充分利用 DNS 转发器。该功能将 DNS 请求转发到外部服务器。如果 DNS 服务器无法在其区域中找到资源记录，可以将请求发送给另一台 DNS 服务器，以进一步尝试解析。一种常见情况是配置到我们的 ISP 的 DNS 服务器的转发器。

（1）单击“开始”，指向“管理工具”，然后单击“DNS”。

（2）右击“ServerName”， ServerName 是服务器的名称，然后单击“转发器”选项卡。

（3）单击“DNS 域”列表中的一个 DNS 域，或者单击“新建”按钮，在“DNS 域”框中键入希望转发查询的 DNS 域的名称，然后单击“确定”按钮。

（4）在所选域的转发器 IP 地址框中，键入希望转发到的第一个 DNS 服务器的 IP 地址，然后单击“添加”按钮。

（5）重复步骤（4），直到所有希望转发都被添加到 DNS 服务器中。

（6）单击“确定”按钮。

5．配置根提示

Windows 可以使用根提示。根提示资源记录可以存储在 Active Directory 或文本文件（%SystemRoot%/System32/DNS/Cache.dns）中。Windows 使用标准的 InterNIC（Internet 信息中心）根服务器。另外，当运行 Windows Server 2003 的服务器查询根服务器时，它将用最新的根服务器列表更新自身。

（1）单击“开始”，指向“管理工具”，然后单击“DNS”。

（2）右击“ServerName”，ServerName 是服务器的名称，然后单击“属性”，单击“根提示”选项卡。DNS 服务器的根服务器在名称服务器列表中列出。

5.5 DHCP的配置

5.5.1 DHCP的基本概念

动态主机配置协议（Dynamic Host Configuration Protocol, DHCP）是一个局域网的网络协议，使用 UDP 协议工作，主要有两个用途：为内联网或网络服务供应商自动分配 IP 地址给用户；以及将其作为内联网管理员对内联网中所有计算机的中央管理手段。

DHCP 是一种使网络管理员能够集中管理和自动分配 IP 网络地址的通信协议。在 IP 网络中，每个连接 Internet 的设备都需要分配惟一的 IP 地址。DHCP 使网络管理员能从中心节点监控和分配 IP 地址。当某台计算机移到网络中的其他位置时，能自动收到新的 IP 地址。

DHCP 使用了租约（或称为计算机 IP 地址的有效期）的概念。租用时间是不定的，主要取决于用户在某地连接 Internet 需要的时间，这对于教育行业和其他用户频繁改变的环境是很实用的。通过较短的租期，DHCP 能够在一个计算机比可用 IP 地址多的环境中动态地重新配置网络。

DHCP 支持为计算机分配静态地址，如需要永久性 IP 地址的 Web 服务器。

DHCP 客户端是装在计算机中的一个程序，一般的操作系统都默认安装了 DHCP 的客户端，这样用户就可以对其进行配置操作。

5.5.2 配置DHCP

1．安装前的注意事项

（1）DHCP 服务器本身必须采用固定的 IP 地址。

（2）规划 DHCP 服务器的可用 IP 地址。

（3）确保系统中已经安装了 DHCP 服务并能正常运行（判定方法与 DNS 服务类似）。

2．添加 DHCP 服务器

在安装 DHCP 服务后，用户必须首先添加一个授权的 DHCP 服务器，并在服务器中添加作用域设置相应的 IP 地址范围及选项类型，以便 DHCP 客户机在登录到网络时，能够获得 IP 地址租约和相关选项的设置参数。添加 DHCP 服务器的步骤如下：

（1）在“管理工具”菜单启动 DHCP 管理控制台（如图 5.22 所示）。

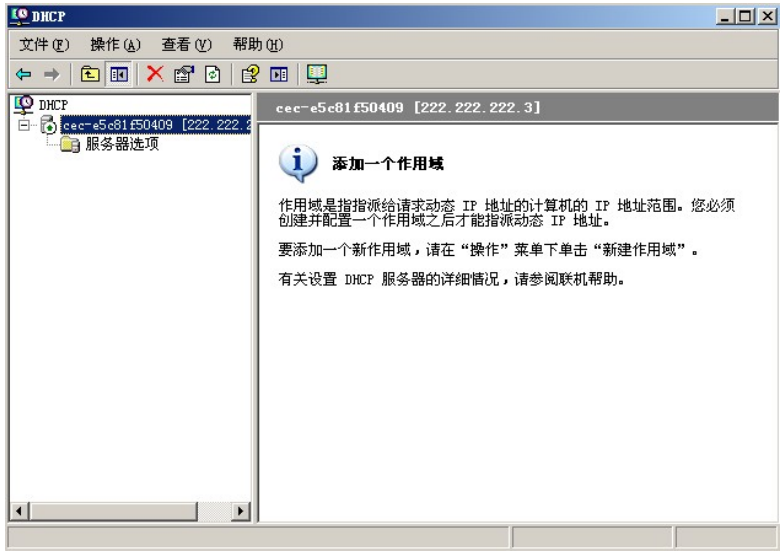


图 5.22 DHCP 管理控制台

（2）选择“操作”菜单中的“添加服务器”，启动添加服务器向导；单击“下一步”按钮出现“指定 DHCP 服务器”对话框；单击“浏览”按钮后出现“目录中授权的服务器”对话框，用户可给 DHCP 服务器添加授权；单击“添加”按钮，出现“授权 DHCP 服务器”窗口，填写用户要建立 DHCP 服务的服务器名或 IP 地址。

（3）在“目录中授权的服务器”对话框中，选择上一步添加的服务器，单击“管理”按钮→单击“下一步”按扭→完成。

（4）在 DHCP 管理控制台中出现刚才添加的服务器。

3．在DHCP服务器中添加作用域

（1）在 DHCP 管理控制台中单击要添加作用域的服务器→单击“操作”菜单→“新建作用域向导”。

（2）单击“下一步”按钮，在“输入作用域名”对话框中输入本域的域名。

（3）单击“下一步”按钮，输入作用域将分配的地址范围及子网掩码。

（4）单击“下一步”按钮，在“添加排除”对话框中输入需要排除的地址服务。

（5）单击“下一步”按钮，选择租约期限（默认为 8 天）。

（6）单击“下一步”按钮，选择配置 DHCP 选项。

（7）单击“下一步”按钮，输入默认网关 IP 地址。

（8）输入域名称和 DNS 服务器的 IP 地址。

（9）单击“下一步”按钮，添加 WINS 服务器的地址。

（10）单击“下一步”按钮，选择激活作用域。

（11） 在 DHCP 管理控制台中出现新添加的作用域，在 DHCP 控制台右侧窗体中的状态条中显示“运行中”表示作用域已启用。

（12）设置完毕，当 DHCP 客户机启动时，可以从 DHCP 服务器获得 IP 地址租约及选项设置。在 DHCP 管理控制台中，作用域下多了下列四项。

① 地址池：用于查看、管理现在的有效地址范围和排除范围。

② 地址租约：用于查看、管理当前的地址租用情况。

③ 保留：用于添加、删除特定保留的 IP 地址。

④ 作用域选项：用于查看、管理当前作用域提供的选项类型及其设置值。

5.6 FTP服务的配置

5.6.1 FTP服务概述

文件传输协议（File Transfer Protocol，FTP）是用于在网络上进行文件传输的一套标准协议。它属于网络协议组的应用层。

FTP 能操作任何类型的文件而不需要进一步处理，就像 MIME 或 Unicode 一样。但是，FTP 有着极高的延时，这意味着，从开始请求到第一次接收需求数据之间的时间会非常长；并且经常必须执行一些冗长的登录进程。

FTP 服务一般运行在 20 和 21 两个端口。端口 20 用于在客户端和服务器之间传输数据流，而端口 21 用于传输控制流，并且是命令通向 FTP 服务器的进口。当数据通过数据流传输时，控制流处于空闲状态。当控制流空闲很长时间后，客户端的防火墙会将其会话置为超时，这样当大量数据通过防火墙时，会产生一些问题。此时，虽然文件可以成功地传输，但因为控制会话，会被防火墙断开；传输会产生一些错误。

FTP 实现的目标为：促进文件的共享（计算机程序或数据），鼓励间接或者隐式地使用远程计算机，向用户屏蔽不同主机中各种文件存储系统（File System）的细节；可靠和高效地传输数据。

缺点：密码和文件内容都使用明文传输，可能会被窃听；因为必须开放一个随机的端口以建立连接，当防火墙存在时，客户端很难过滤处于主动模式下的 FTP 流量。这个问题，通过使用被动模式的 FTP，得到了很大解决；服务器可能会被告知连接一个第三方计算机的保留端口；FTP 虽然可以被终端用户直接使用，但它设计成被 FTP 客户端程序控制；运行 FTP 服务的许多站点都开放匿名服务，在这种设置下，用户不需要账号就可以登录服务器，默认情况下，匿名用户的用户名是 “anonymous”。这个账号不需要密码，虽然通常要求输入用户的邮件地址作为认证密码，但这只是一些细节或者此邮件地址根本不被确定，而是依赖于 FTP 服务器的配置情况。

5.6.2 配置FTP服务器

1．配置前的注意事项

由于 FTP 依赖 Microsoft Internet 信息服务 （IIS），因此计算机上必须安装 IIS 和 FTP 服务。

2．配置 FTP 服务

（1）启动“Internet 信息服务管理器”或打开 IIS 管理单元。

（2）展开“服务器名称”，其中服务器名称是该服务器的名称。

（3）展开“FTP 站点”。

（4）右击“默认 FTP 站点”，然后单击“属性”。

（5）在如图 5.23 所示的对话框中，选择“安全账户”选项卡。

（6）选中“允许匿名连接”复选框（如果它尚未被选中），然后选中“仅允许匿名连接”复选框。

（7）如果选中“仅允许匿名连接”复选框，则应将 FTP 服务配置为仅允许匿名连接。用户无法使用用户名和密码登录。

（8）单击“主目录”选项卡。

（9）选中“读取”和“日志访问”复选框（如果它们尚未被选中），然后清除“写入”复选框（如果它尚未被清除）。

（10）单击“确定”按钮。

（11）退出“Internet 信息服务管理器”或者关闭 IIS 管理单元。

FTP 服务器现已配置为接受传入的 FTP 请求。将要提供的文件复制或移动到 FTP 发布文件夹以供访问。默认的文件夹是驱动器:\Inetpub\Ftproot，其中驱动器是安装 IIS 的驱动器。

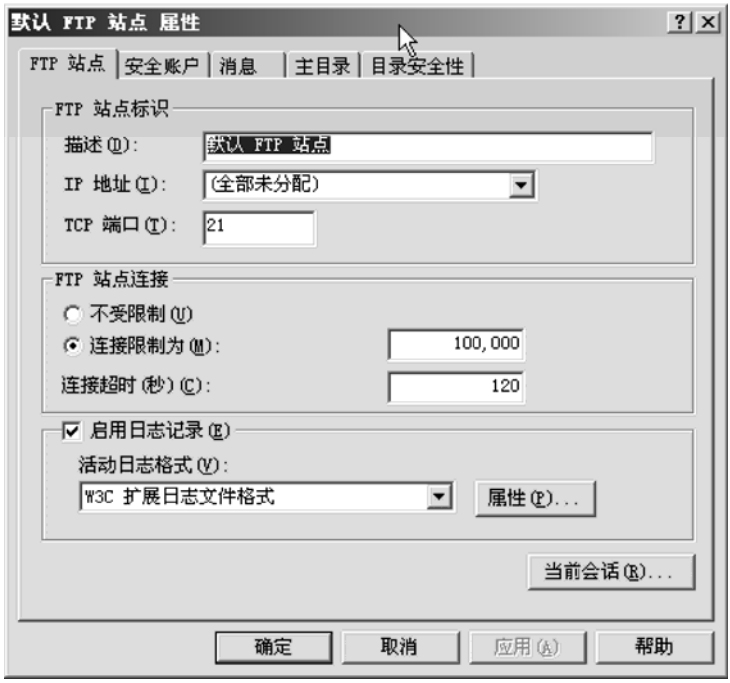


图 5.23 FTP 服务的配置

5.7 WWW服务的配置

5.7.1 WWW服务概述

万维网（也称为“Web”、“WWW”、“W3”，英文全称为“World Wide Web”），是一个由许多互相链接的超文本文档组成的系统，通过 Internet 访问。在这个系统中，每个有用的事物，称为一种“资源”；并且由一个全域“统一资源标志符”（URI）标志；这些资源通过超文本传输协议（Hypertext Transfer Protocol）传送给使用者，而后者通过单击链接来获得资源。万维网联盟（World Wide Web Consortium，W3C），又称为 W3C 理事会，于 1994 年 10 月在麻省理工学院（MIT）计算机科学实验室成立。万维网常被当成互联网的同义词，这是一种误解，万维网是依靠互联网运行的一项服务。

从狭义上讲，WWW 服务就是 HTTP 服务，HTTP 是一个客户端和服务器端请求和应答的标准（TCP）。客户端是终端用户，服务器端是网站。客户端用户通过使用 Web 浏览器、网络爬虫或者其他的工具来访问服务器端。

通常，由 HTTP 客户端发起一个请求，建立一个到服务器指定端口（默认是 80 端口）的 TCP 连接。HTTP 服务器则在那个端口监听客户端发送过来的请求。一旦收到请求，服务器（向客户端）发回一个状态行（如“HTTP/1.1 200 OK”）和（响应的）消息，消息的消息体可能是请求的文件、错误消息或者其他信息。

5.7.2 配置WWW服务器

1．配置前的准备

确保服务器上已经安装了 IIS 且正常运行。如果没有安装，则应通过“添加和删除程序”→“Windows 组件”启动安装。

2．基本Web站点配置

（1）单击“开始”，指向“管理工具”，然后单击“Internet 信息服务（IIS）”。

（2）展开“服务器名称”，然后展开“Web 站点”。

（3）右键单击“默认 Web 站点”，然后单击“属性”。

（4）单击“网站”选项卡。如果已为计算机分配了多个 IP 地址，则在“IP 地址”框中单击要指定给此 Web 站点的 IP 地址。

（5）单击“性能”选项卡。在该选项卡中可设置影响内存、带宽使用和 Web 连接数量的属性（每个浏览 Web 站点的客户机通常都使用大约三个连接）。

（6）单击“主目录”选项卡。如果想使用存储在本地计算机上的 Web 内容，则选中“此计算机上的目录”单选钮（如图 5.24 所示），然后在“本地路径”框中键入想要的路径；如果要使用存储在另一台计算机上的 Web 内容，则单击“另一台计算机上的共享”单选钮，然后在显示的“网络目录”框中键入所需位置；如果要使用存储在另一个 Web 地址的 Web 内容，则选中“重定向到 URL”单选钮，然后在“重定向到”框中键入所需位置。在“客户会送到”下，选中相应的复选框。

（7）单击“文档”选项卡。请注意，可由 IIS 作为默认启动文档的文档列表。如果要使用 Index.html 作为启动文档，就必须添加它。添加方法是：单击“添加”按钮，在“添加默认文档”对话框中，键入 Index.html，然后单击“确定”按钮。单击向上箭头按钮，直到 Index.html

显示在列表的顶部。

（8）单击“确定”按钮，关闭“默认 Web 站点属性”对话框。

（9）右键单击“默认 Web 站点”，然后单击“权限”按钮。

（10）请注意，在此 Web 站点上具有操作权限的用户账户。单击添加其他可操作此 Web 站点的用户账户。

（11）单击“确定”按钮，返回到“Internet 信息服务”窗口。

（12）右键单击“默认 Web 站点”，然后单击“停止”按钮。

（13）右键单击“默认 Web 站点”，然后单击“开始”按钮。

现在，该服务器已配置为接受传入的访问默认 Web 站点的 Web 请求。用户可以将默认 Web 站点的内容替换为想要的 Web 内容，或者创建新 Web 站点。

3．配置匿名身份验证

为保证互联网上的用户都能访问服务器上的资源，要配置匿名身份验证，请按以下步骤操作：

（1）打开“Internet 信息服务（IIS）”窗口，展开要配置的 Web 站点，然后单击“属性”。

（2）在“默认 Web 站点属性”对话框中，单击“目录安全性”选项卡。

（3）在“身份验证和访问控制”下，单击“编辑”按钮。

（4）选中“启用匿名访问”复选框。

备注：“用户名”框中的用户账户只用于通过 Windows guest 账户进行匿名访问。

在默认情况下，服务器会创建并使用账户 IUSR_computername。匿名用户账户密码仅在 Windows 中使用，匿名用户不使用用户名和密码登录。

（5）在“已验证身份的访问”下，选中“集成的 Windows 身份验证”复选框。

（6）单击“确定”按钮两次，完成配置。

图 5.24　Web 站点主目录的配置

5.8 管理远程桌面

远程桌面协议（Remote Desktop Protocol，RDP）是一个多通道（Multichannel）协议，让用户（用户端或称“本地计算机”）连上提供微软终端机服务的计算机（服务器端或称“远程计算机”）。大部分 Windows 都有用户端所需的软件。借助这些软件，任何用户都可以轻松实现对服务器的远程访问和管理。如果要让它更好地为用户服务，则需要使用“组策略编辑器”对“远程桌面”做进一步的设置。下面将介绍使用“组策略编辑器”对“远程桌面”设置的知识。

如果要打开“组策略编辑器”窗口，请单击“开始”→“运行”，在“运行”对话框中键入“gpedit.msc”命令并回车，即可打开“组策略编辑器”窗口。

1．允许/禁止“远程桌面”连接

可以通过组策略允许或禁止使用“远程桌面”连接功能。在“组策略编辑器”窗口左侧，依次展开“计算机配置”→“管理模板”→“Windows 组件”→“终端服务”目录。单击目录名“终端服务”，在窗口右侧双击“允许用户使用终端服务远程连接”选项。然后，在如图 5.25 所示的对话框的“设置”选项卡中选中“已启用”或“已禁用”单选钮并单击“确定”按钮。

2．配置“数据重定向”

通过配置客户端/服务器数据重定向，可以设置在建立连接后所能使用的客户端资源。双击目录名“客户端/服务器数据重定向”，在窗口右侧中列出了可以设置的客户端资源。假如想在成功建立“远程桌面”连接后使用客户端的声卡播放服务器上的声音文件，则应该双击“允许音频重定向”选项，在如图 5.25 所示的对话框的“设置”选项卡中选中“已启用”选项并单击“确定”按钮。

图 5.25　远程桌面的配置

3．设置空闲会话连接时间

在成功建立连接后，可能由于某种原因（如忘记断开连接）致使会话处于空闲状态，很明显这是不安全的。不过，可以限制空闲会话的连接时间。展开“会话”子目录，双击其中的“为活动但空闲的终端服务会话设置时间限制”选项，打开如图 5.25 所示的对话框，在“设置’选项卡中选中“已启用”选项，在“空闲会话限制”下拉列表框中选中一个时间选项（如“5 分钟”），并单击“确定”按钮。

4．添加远程访问用户

在实际工作中，需要使用“远程桌面”功能的可能不止系统管理员一个人。因此，可以为有这方面需求的用户设置权限。设置方法如下：

右键单击“我的电脑”，选择“属性”命令，在“系统属性”对话框的“远程”选项卡中单击“选择远程用户”按钮。然后在“远程桌面用户”对话框中单击“添加”按钮，在“选择用户”对话框中依次单击“高级”→“立即查找”按钮。从用户列表中选中目标用户。

5.9 活动目录的配置

5.9.1 域林的规划

在安装活动目录之前，首先要对活动目录的结构进行细致的规划设计，让用户和管理员在使用时更为方便。

1．规划DNS

如果用户准备使用活动目录，则需要首先规划名称空间。当 DNS 域名称空间可在 Windows 2003 中正确执行之前，需要有可用的活动目录结构。因此，从活动目录设计着手并用适当的 DNS 名称空间支持它。

在 Windows 2003 中，用 DNS 名称命名活动目录域。选择 DNS 名称用于活动目录域时，以保留在 Internet 上使用的已注册 DNS 域名后缀开始（如 microsoft.com），并将该名称和单位中使用的地理（部门）名称结合起来，组成活动目录域的全名。例如，Microsoft 的 Sales 组可能称其域为“sales.microsoft.com”。这种命名方法确保每个活动目录域名是全球惟一的。而且，这种命名方法一旦被采用，使用现有名称作为创建其他子域的父名称以及进一步增大名称空间以供单位中的新部门使用的过程将变得非常简单。

2．规划用户的域结构

最容易管理的域结构就是单域。规划时，用户应从单域开始，并且只有在单域模式不能满足用户的要求时，才增加其他域。单域可跨越多个地理站点，并且单个站点可包含属于多个域的用户和计算机。在一个域中，可以使用组织单元（Organizational Units，OU）来实现这个目标。然后，可以指定组策略设置并将用户、组和计算机放在组织单元中。

3．规划用户的委派模式

用户可以将权限下派给单位中最底层的部门，方法是在每个域中创建组织单元树，并将部分组织单元子树的权限委派给其他用户或组。通过委派管理权限，用户不再需要那些定期登录到特定账户的人员，这些账户具有对整个域的管理权。尽管用户还拥有整个域的管理授权的管理员账户和域管理员器组，但仍保可以留这些账户以备少数管理员偶尔使用。

5.9.2 活动目录的配置

1．成员服务器和独立服务器

Windows Server 2003 服务器在域中可以充当三种角色：域控制器、成员服务器和独立服务器。当一台 Windows Server 2003 成员服务器安装了活动目录后，服务器就成为域控制器，域控制器可以对用户的登录等进行验证。当 Windows Server 2003 成员服务器可以仅加入到域中，而不安装活动目录时，服务器的主要目的是提供网络资源，这样的服务器称为成员服务器，也可以称为现有域中的附加域控制器。独立服务器和域没有什么关系，如果服务器不加入到域中也不安装活动目录，就称为独立服务器。

服务器的三个角色可以发生改变：例如删除活动目录，使服务器成为成员服务器还是独立服务器，取决于该服务器的域控制器类型。如果要删除活动目录的服务器不是域中惟一的域控制器，则删除活动目录将使该服务器成为成员服务器；如果要删除活动目录的服务器是域中最后一个域控制器，则删除活动目录使该服务器成为独立服务器。同时，独立服务器也可以提升为成员服务器。

注意：在安装活动目录之后，不但服务器的开机和关机时间变长，而且系统的执行速度也变慢。如果用户对某个服务器没有特别要求或不把它作为域控制器来使用，则可将该服务器上的活动目录删除，使其降级成为成员服务器或独立服务器。

2．创建子域

子域这个名称是相对的，创建子域必须使用具有充分权限的用户账户登录域控制器，被提升为子域的计算机必须是已加入域的成员，并且以 Active Directory 中 Domain Admins 组或 Enterprise Admins 组的用户账户登录到域控制器，否则将会被提示无权提升域控制器。

操作系统版本的兼容性：被提升为子域控制器的计算机必须安装 Windows Server 2003（Windows Server 2003 Web Edition 除外）或 Windows Server2000 操作系统。

正确配置 DNS 服务器：必须将当前计算机的 DNS 服务器指向主域控制器，并且保证域控制器的 DNS 已经被正确配置，否则将会被提示无法联系到 Active Directory 域控制器。

域名长度：Active Directory 域名最多包含 64 个字符或 155 个字节。

3．创建备份域控制器

通常，一个功能强大的网络中至少应设置两台域控制器，即一台主域控制器和一台备份域控制器。网络中的第一台安装活动目录的服务器通常会被默认设置为主域控制器；其他域控制器（可以多台）称为备份域控制器，主要用于主域控制器出现故障时及时接替工作，继续提供各种网络服务，以不致造成网络瘫痪。另外，备份域控制器还可以起到备份数据的作用。

4．创建信任关系

信任关系是两个域控制器之间实现资源互访的重要前提，任何一个域被加入到域目录树后，这个域都会自动信任父域，同时父域也会自动信任这个新域，而且这些信任关系具备双向传递性。由于这个信任关系的功能是通过 Kerberos 安全协议完成的，因此有时也被称为 Kerberos 信任。

当网络中有多个不同的域，想要让每个用户都可以自由访问网络中的每台服务器（不管用户是否属于这个域）时，域之间需要创建信任关系。

本 章 小 结

本章介绍了 Windows 服务器上常用的应用服务的配置与管理，同时也介绍了 Windows 网络系统本身的一些基本配置工作，如用户和组账号、NTFS 权限配置等。

（1）Windows 网络中有两种主要的账号类型：域用户账号和本地账号。

（2）成员服务器提升为域控制器后，就无法使用“本地用户和组”查看本地用户和组账户。

（3）要使用 NTFS 的权限管理功能，要求被管理的磁盘分区必须是 NTFS 格式的。Windows NT 以前版本的 Windows 无法识别 NTFS 格式的分区。

（4）在以 NT 内核为基础的 Windows 中，权限主要分为七大类：完全控制、修改、读取和运行、列出文件夹目录、读取、写入、特别的权限。

（5）域名和 DNS 服务两者缺一不可。每个域名必然对应一个 IP 地址。

（6）动态主机配置协议（DHCP）是一种使网络管理员能够集中管理和自动分配 IP 网络地址的通信协议。

（7）FTP 依赖 Microsoft Internet 信息服务（IIS），因此计算机上必须安装 IIS 和 FTP 服务。

（8）WWW 服务使用 HTTP 协议，客户端使用 Web 浏览器访问 WWW 服务器。使用“统一资源标志符（URI）”标志 WWW 上的所有资源。

（9）目录服务，如 Active Directory，提供了用于存储目录数据并使该数据可由网络用户和管理员使用的方法。

（10）活动目录和 DNS 密不可分，它使用 DNS 服务器来登记域控制器的 IP、各种资源的定位等，因此在一个域林中至少存在一个 DNS 服务器。

（11）一个域林在实施前，要先进行周密的规划和设计。

思 考 题

1．Windows 2003 的用户账户管理分为哪几种？有什么区别？

2．DHCP 服务器传送给 DHCP 客户的基本网络参数有哪几个？

3．域名服务器主要提供哪几种解析服务？

4．DNS 系统的结构是如何组织的？

5．在规划域林时应注意什么？

实训 5——配置DNS、DHCP和WINS服务器

一、实训目的

1．了解 DNS、DHCP 和 WINS 配置的实际过程。

2．熟悉常见网络服务的作用。

二、实训环境

某公司拥有 5 台计算机，通过主机获取动态 TCP/IP 配置上网，网络协议配置及地址如表 5.2 所示。

表 5.2　网络协议配置及地址

网 络 协 议	地　　址
IP 地址范围	211.83.34.41 至 211.83.34.48
DHCP 服务主机地址	211.83.34.42
DNS 服务地址	211.83.32.42
路由/网关地址	211.83.34.41
WINS 服务地址	211.83.34.42

三、实训要求

1．正确分配 IP 地址。

2．正确配置各服务。

四、实训步骤

1．DHCP 的配置：

因 211.83.34.41 和 211.83.34.42 已经分配给网关和服务器，故在分配动态地址后应排除这两个地址。

（1）打开 DHCP 控制程序。

（2）添加一个与本机同名的 DHCP 服务器。

（3）新建一个作用域来指派动态 IP 地址。

① 在“起始 IP 地址”和“结束 IP 地址”中分别输入 211.83.34.41 和 211.83.34.48。

② 将网关的地址 211.83.34.41 和服务器地址 211.83.34.42 排除。

③ 为分配给客户端的这些 IP 地址设定一个有限期。

④ 在“路由器（默认网关）”中输入网关地址 211.83.34.41。

⑤ 在“DNS 服务器”中输入 DNS 服务器的地址 211.83.34.42。

⑥ 在“WINS 服务器”中输入 WINS 服务器的地址 211.83.34.42。

2．DNS 的配置：

（1）打开 DNS 的配置程序。

（2）新建一个名为“lab.cec.edu.cn”的正向搜索区域，并将其设置为“标准主要区域”。

（3）新建一个名为“lab.cec.edu.cn”的反向搜索区域，并将其设置为“标准主要区域”。

3．WINS 的配置：

（1）打开 WINS 的配置程序。

（2）添加一个与本机同名的 WINS 服务器。

实训 6——配置WWW、FTP服务器

一、实训目的

掌握 WWW、FTP 服务器的安装、配置和管理的方法。

二、实训环境

1．服务端：安装 Windows Server 2003 操作系统，并准备 Windows Server 2003 的安装光盘。

2．客户端：Windows 2000/2003 等操作系统。

3．连接客户机与服务器的局域网。

三、实训要求

1．安装、配置 WWW 和 FTP 服务。

2．测试 WWW 和 FTP 服务。

四、实训步骤

1．安装 WWW 服务。

（1）进入“控制面板”。

（2）双击“添加或删除程序”。

（3）单击“添加/删除 Windows 组件”。

2．在“组件”列表框中，双击“应用程序服务器”。

（1）双击“Internet 信息服务（IIS）”。

（2）选择“万维网服务”及“文件传输协议（FTP）服务”。

（3）双击“万维网服务”，选择“Active Server Pages”及“万维网服务”等。

3．配置 WWW 服务。

（1）单击“开始”，指向“管理工具”，单击“Internet 信息服务（IIS）管理器”。

（2）在“Internet 信息服务（IIS）管理器”窗口中双击“本地计算机”。

（3）右击“网站”，在弹出的菜单中选择“新建”→“网站”，打开“网站创建向导”。

（4）依次填写“网站描述”、“IP 地址”、“端口号”、“路径”和“网站访问权限”等。

（5）为了便于访问，还应设置默认文档（Index.asp、Index.htm）。

4．在客户机上通过 Intranet 网络验证上述 WWW 服务配置的正确性。

5．安装 FTP 服务。

（1）单击“开始”，指向“控制面板”，然后单击“添加或删除程序”。

（2）单击“添加/删除 Windows 组件”。

（3）在“组件”列表中，单击“应用程序服务器”，单击“Internet 信息服务（IIS）”（但是不要选中或清除复选框），然后单击“详细信息”。

（4）选中下列复选框（如果它们尚未被选中）：公用文件、文件传输协议 （FTP） 服务、Internet 信息服务管理器。

（5）选中你想要安装的任何其他的 IIS 相关服务或子组件旁边的复选框，然后单击“确定”按钮。

（6）单击“下一步”按钮。

（7）出现提示时，请将 Windows Server 2003 CD-ROM 插入计算机的 CD-ROM 或 DVD-ROM 驱动器，或提供文件所在位置的路径，然后单击“确定”按钮。

（8）单击“完成”按钮。

6．配置 FTP 服务。

（1）启动“Internet 信息服务管理器”或打开 IIS 管理单元。

（2）展开“服务器名称”，其中服务器名称是该服务器的名称。

（3）展开“FTP 站点”。

（4）右击“默认 FTP 站点”，然后单击“属性”。

（5）单击“安全账户”选项卡。

（6）选中“允许匿名连接”复选框（如果它尚未被选中），然后选中“仅允许匿名连接”复选框。如果选中“仅允许匿名连接”复选框，则将 FTP 服务配置为仅允许匿名连接。用户无法使用用户名和密码登录。

（7）单击“主目录”选项卡。

（8）选中“读取”和“日志访问”复选框（如果它们尚未被选中），然后清除“写入”复选框（如果它尚未被清除）。

（9）单击“确定”按钮。

（10）退出“Internet 信息服务管理器”或者关闭 IIS 管理单元。

7．测试 FTP 服务。

FTP 服务器现已配置为接受传入的 FTP 请求。将要提供的文件复制或移动到 FTP 发布文件夹以供访问。默认的文件夹是驱动器:\Inetpub\Ftproot，其中驱动器是安装 IIS 的驱动器。

实训 7——配置活动目录

一、实训目的

掌握活动目录的配置方法，加深对活动目录、域、信任等概念的理解。

二、实训环境

6 台安装了 Windows Server 2003 企业版的独立服务器。

三、实训内容

某公司的域林拓扑图如图 5.26 所示。

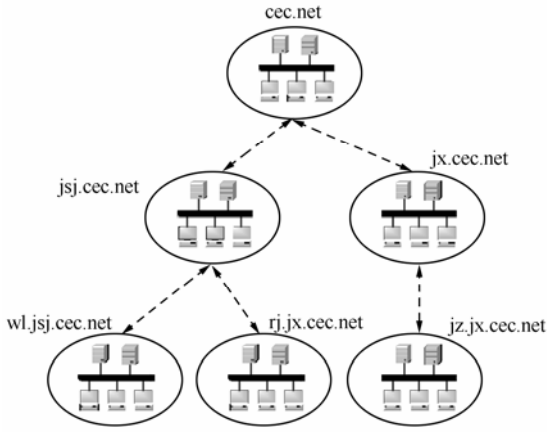


图 5.26　某公司的域林拓扑图

分别安装 6 台 Windows Server 2003 独立服务器，要求这 6 台服务器在同一个局域网中，并进行分别设置：

1．计算机 WIN2003A，IP 地址为 192.168.0.1，子网掩码为 255.255.255.0，首选 DNS 服务器为 192.168.0.1，在服务器上安装域名为 cec.net 的域控制器。

2．计算机 WIN2003B，IP 地址为 192.168.0.2，子网掩码为 255.255.255.0，首选 DNS 服务器为 192.168.0.1，在服务器上安装域名为 jsj.cec.net 的额外域控制器。

3．计算机 WIN2003C，IP 地址为 192.168.0.3，子网掩码为 255.255.255.0，首选 DNS 服务器为 192.168.0.1，在服务器上安装域名为 jx.cec.net 的额外域控制器。

4．计算机 WIN2003D，IP 地址为 192.168.0.4，子网掩码为 255.255.255.0，首选 DNS 服务器为 192.168.0.1，在服务器上安装域名为 wl.jsj.cec.net 的额外域控制器。

5．计算机 WIN2003E，IP 地址为 192.168.0.5，子网掩码为 255.255.255.0，首选 DNS 服务器为 192.168.0.1，在服务器上安装域名为 rj.jsj.cec.net 的额外域控制器。

6．计算机 WIN2003F，IP 地址为 192.168.0.6，子网掩码为 255.255.255.0，首选 DNS 服务器为 192.168.0.1，在服务器上安装域名为 jz.jx.cec.net 的额外域控制器。

分别为上述 6 个域建立如图 5.26 所示的域林拓扑图的信任关系。

四、实训步骤

1．在 WIN2003A 中安装域控制器，步骤与实训 3 相同，在此略去。

2．在另外 5 台计算机中安装额外域控制器的方法如下：

（1）启动 Active Directory 安装向导，如果想从备份中复制活动目录数据库，则可以直接运行“dcpromo/adv”命令。

（2）当 Active Directory 安装向导运行至“域控制器类型”窗口时，需要选中“现有域的额外域控制器”单选钮，将该计算机设置为额外域控制器。

注意：一旦将该计算机升级为额外域控制器后，原有的本机账户将被删除，密钥（Cryptographic Keys）也将被删除，因此，应当先进行备份。另外，已被加密的数据（如文件和电子邮件）也将无法读取，应当先将这些数据解密并备份。

（3）单击“下一步”按钮，在“网络凭据”窗口中，输入拥有将计算机升级为域控制器权限的用户名和密码。该用户名必须隶属于目的域的 Domain Admins 组、Enterprise Admins 组，或者是其他授权用户。其他安装过程，请参见实训 3“Windows Server 2003 活动目录的安装”的相关内容。

3．创建信任关系。

下面以 cec.cn 和 jsj.cec.cn 这两个域为例，介绍信任关系的创建。创建信任关系时，在 WIN2003A 计算机上进行操作，具体的操作步骤为：

（1）单击“开始”→“管理工具”→“Active Directory 域和信任关系”，从主窗口中右击 cec.cn 域名，从出现的菜单中选择“属性”，打开“域属性”对话框，单击“信任”选项卡。由于当前域尚未与其他任何域建立信任关系，所以此时列表为空。

（2）单击“新建信任”按钮，打开“新建信任向导”，单击“下一步”按钮，弹出“信任名称”对话框，在“名称”文本框中输入要与之建立信任关系的 NetBIOS 名称或者 DNS 名称，这里为“jsj.cec.cn”。

（3）单击“下一步”按钮，弹出“信任方向”对话框，选择信任关系的方向，可以是“双向”、“单向：内传”、“单向：外传”。双向的信任关系实际上是由两个单向的信任关系组成的，因此也可以通过分别建立两个单向的信任关系来建立双向的信任关系。这里为了方便，选择“双向”单选钮，单击“下一步”按钮。

（4）由于信任关系要在一方建立传入，在另一方建立传出，为了方便，选择“这个域和指定的域”单选钮，同时创建传入和传出信任，单击“下一步”按钮，否则必须在 cec.cn 域上重复以上的步骤。

（5）在弹出的对话框中输入 cec.cn 域中管理员的账户和密码，单击“下一步”按钮。

（6）选中“是，确认传出信任”单选钮，即确认 cec.cn 域信任 jsj.cec.cn 域，单击“下一步”按钮。

（7）选中“是，确认传入”单选钮，即确认 jsj.cec.cn 域信任 cec.cn 域，单击“下一步”按钮，成功创建信任关系。此时，在“受此域信任的域”和“信任此域的域”列表框中均可看到刚才创建的信任关系。

重复以上步骤，创建另外 5 组信任关系。

第 6 章　广域网与网络互连技术

本章要点

本章将从广域网的结构、特点和分类入手，介绍典型广域网 PSTN、ISDN、X.25、帧中继和 DDN，并对网络互连技术、典型的网络互连设备（中继器、网桥、路由器和网关等）的功能、交换机的一般配置、路由器的一般配置等内容进行全面的探讨。

本章目标

- 了解广域网的基本概念、特点和分类
- 了解 PSTN、ISDN、X.25、帧中继和 DDN 的概念、特点和应用
- 了解网络互连的概念和目的
- 掌握网络互连设备的作用层次、功能及应用
- 掌握交换机的基本配置
- 了解 VLAN 的概念及配置方法
- 掌握路由器的基本配置
- 掌握静态路由协议和动态路由协议 RIP、OSPF 的基本配置
- 了解广域网协议 PPP、X.25 和帧中继的配置
- 了解 ACL、NAT 的概念及配置

6.1　广域网概述

6.1.1　什么是广域网

广域网（Wide Area Network，WAN）是指覆盖范围广、传输速率相对较低、以数据传输为主要目的的数据通信网。它通过若干个节点交换机和连接这些节点的物理链路将分布在异地的多个局域网或主机连接起来，形成一个范围广泛的远程网络。它通常覆盖一个国家甚至全球，可以使人们最大范围地传送信息和共享资源。

局域网和广域网之间，既有区别又有联系。在技术上，局域网领先于广域网。在应用上，局域网强调的是资源共享；而广域网则着重数据传输。对于局域网，人们更多关注的是如何根据应用需求来规划、建立和应用；对于广域网，侧重的则是网络能够提供什么样的数据传输业务，以及用户如何接入网络等。

6.1.2　广域网的结构

广域网的结构分为通信子网与资源子网，如图 6.1 所示。

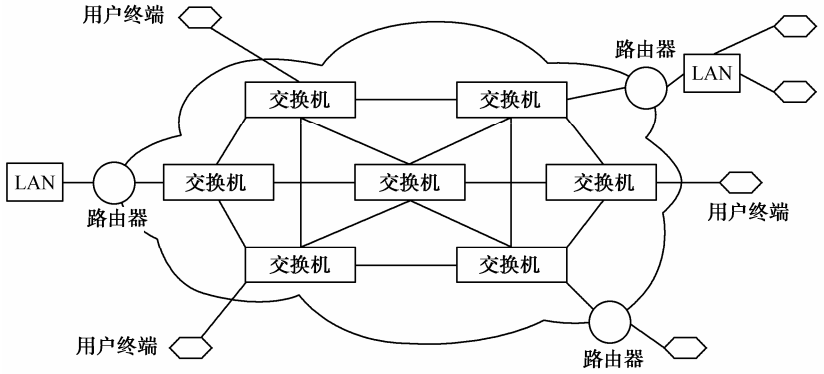


图 6.1　广域网的结构

广域网分为通信子网与资源子网两部分，主要是由一些节点交换机和连接这些交换机的链路组成。节点交换机执行将分组存储转发的功能。广域网的链路一般分为传输主干和末端用户线路，根据末端用户线路和广域网类型的不同，有多种接入广域网的技术，并提供各种接口标准。

6.1.3　广域网的特点

与覆盖范围较小的局域网相比，广域网的特点如下：

（1）覆盖范围广，可达数千公里甚至全球。

（2）广域网没有固定的拓扑结构。

（3）广域网通常使用高速光纤作为传输介质。

（4）局域网可以作为广域网的终端用户与广域网连接。

（5）广域网主干带宽宽，但提供给单个终端用户的带宽窄。

（6）数据传输距离远，往往要经过多个广域网设备转发，延时较长。

（7）广域网管理、维护困难。

6.1.4　广域网的种类

广域网可以分为公共传输网络、专用传输网络和无线传输网络。

（1）公共传输网络一般由政府电信部门组建、管理和控制，网络内的传输和交换装置可以提供（或租用）给任何部门和单位使用。

公共传输网络大体可以分为两类：

① 电路交换网络。主要包括公共交换电话网（PSTN）和综合业务数字网（ISDN）。

② 分组交换网络。主要包括 X.25 分组交换网、帧中继和交换式多兆位数据服务（SMDS）。

（2）专用传输网络是由一个组织或团体自己建立、使用、控制和维护的私有通信网络。一个专用网络起码要拥有自己的通信和交换设备，它可以建立自己的线路服务，也可以向公用网络或其他专用网络进行租用。

专用传输网络主要是数字数据网（DDN）。DDN 可以在两个端点之间建立一条永久的、专用的数字通道。它的特点是在租用该专用线路期间，用户独占该线路的带宽。

（3）无线传输网络主要是移动无线网，典型的有 GSM 和 GPRS 技术等。

6.2 广域网基础与应用

6.2.1 公用电话交换网（PSTN）

1．公用电话交换网概述

公用电话交换网（Public Switching Telephone Network，PSTN）是最早建立的一种大型通信网。PSTN 是向社会提供电话通信服务的公共网络系统，是国家公用通信基础设施之一，由国家电信部门统一建设、管理和运营。它主要提供语音通信服务，同时还提供数据通信业务，如电报、传真、数据交换、可视图片文等。

PSTN 是以模拟技术为基础的电路交换网络。两个数字站通信时，要借助于 MODEM 实现。PSTN 的主要作用是，通过程控交换机之间的连接，实现用户之间在国际、国内范围的语音和数据通信。程控交换机是 PSTN 的核心设备。如果传输和交换的是模拟语音信号，则称为程控模拟交换机；如果传输和交换的是数字语音信号，则称为程控数字交换机。

PSTN 可通过普通电话拨号（用 Com 口或加通信卡，两端用 MODEM 连接），或租用电话专线，或两者经 PSTN 转公用分组数据交换网（X.25 网）等方式与 Internet 连接。

PSTN 具有实时性，租用费用低，入网方式简便、灵活，无存储转发，带宽受限，难于实现不同传输速率设备之间的传输的特点。

2．公用电话换网的组成

从功能角度看，PSTN 由国际交换局、长途交换局、中心交换局、端交换局和用户等层次构成。从通信的覆盖面看，PSTN 又可分成市话通信网、国内长途通信网和国际电话通信网 3 类。

从系统构成角度看，PSTN 由以下部分组成。

（1）传输介质。PSTN 必须拥有提供信息传输的有线（电缆、光缆）或无线（地面微波、卫星）通信介质，并由此构成完整的传输系统。

（2）交换设备。对于 PSTN，交换设备是不可缺少的，它反映并决定了 PSTN 的接续能力，主要有程控交换机、计算机交换机等。

（3）用户设备。用户设备是 PSTN 系统的信源和信宿设备，是用户直接接触和使用的。

（4）信令系统。信令系统是为实现用户通信，在交换局间提供的以呼叫建立、释放为主的各种控制信息的系统。

6.2.2 综合业务数字网（ISDN）

1．ISDN的概念

1984 年 10 月，国际电信联盟（CCITT）推荐的 CCITT ISDN 标准中给出了 ISDN 的定义：“ISDN 是由综合业务数据电话网发展起来的一个网络，它提供端到端的数据连接以支持广泛的服务，包括语音的和非语音的。用户的访问是通过少量、多用途的网络标准实现的。”

简言之，ISDN 是对模拟音频电话系统（PSTN）的再设计，它将决定用户设备与全局网络的连接，能方便地用数字的形式来处理声音、传真、影像和图像通信。

ISDN 网络具有多种功能，包括电路交换、分组交换、无交换连接和公共信道信令功能等。

2．ISDN用户-网络接口

1）ISDN 接口标准

CCITT（ITU）为 ISDN 接口标准定义了 B、D、H 三种通道。B 通道速率为 64kbps，可提供

电路交换、分组交换和半固定线路，用于电话交换业务、X.25 交换业务和租用线路；D 通道速率为 16kbps 或 64kbps，主要用于传送信道信令，也可用于传送分组数据或低速数据；H 通道用于支持高速数据业务，可提供三种速率：H0 为 384kbps，H11 为 1536kbps，H12 为 1920kbps。

2）N-ISDN 的两类接口

N-ISDN 提供两种不同速率的标准接口：一种是基本入口（BRI），速率为 144kbps，支持 2 条 64kbps 的用户信道和 1 条 16kbps 的信令信道；另一种是一次群速率入口（PRI），其速率和 PCM 一次群的速率相同（2048kbps/1544kbps），支持 30 条或 24 条 64kbps 的用户信道和 1 条 64kbps 的信令通道。

在 BRI 和 PRI 中，B 通道是一种数据承载信道，可单独使用，分别以 64kbps 速率传送数据，也可将两个以上 B 信道捆绑在一起以 N×64kbps 的速率使用。

3．B-ISDN

随着数据通信业务向多样化、高速化、综合化的方向发展，用户对数据、图像、传真等业务的要求也越来越高。N-ISDN 受其设计限制，已经越来越不适应未来的发展需求，具体表现在：带宽窄、业务综合能力有限、网络资源利用率不高。

正是因为 N-ISDN 的这些缺点，20 世纪 80 年代出现了一种全新的以异步传输模式（ATM）为核心的 B-ISDN。B-ISDN 是一个高速、异步、时分、复用的综合业务数字网。它提供各种实时高带宽业务，支持电视网、DDN 网和 N-ISDN 网，还能方便有效地提供可变速率业务，支持数据、语音和视频的综合服务。它的特点是可以灵活地支持现有的和将来可能出现的各种业务，能达到很高的网络资源利用率。

虽然 B-ISDN 能提供 135Mbps 以上的接口速率，能实现语音、数据和视频图像的高速传输，但是由于其技术复杂，投资巨大，而且错过了发展的黄金时期，所以目前仍未体现出它的实用价值。

6.2.3 公共分组交换数据网（X.25 网）

公共分组交换数据网是一种采用分组交换技术的数据通信网。它提供的功能相当于 OSI 参考模型的低三层（物理层、数据链路层、网络层）的功能。ITU-T 的 X.25 协议就是针对分组交换网制定的，因此，此类网络也称为 X.25 网。

1．什么是分组交换

分组交换采用存储/转发交换技术，分组是交换处理和传送的对象。先将发送端发送的数据分成固定长度的分组，然后在网络中经各分组交换机逐级“存储/转发”，最终到达接收端。分组交换数据网提供数据报和虚电路两类服务。

（1）数据报服务。数据报服务类似于邮政信件传递方式，每个分组独立地存储和转发，中间节点接收到分组后，首先暂存该分组，然后从不同的路径将分组转发出去，到达目的节点。

（2）虚电路服务。虚电路服务类似于电话网采用的交换方式，在发送数据之前，需要在发方和收方之间建立一条逻辑电路（即虚电路），然后在这条虚电路上传输分组，传输完毕后需要拆除虚电路。

2．X.25 协议

X.25 协议是 CCITT 关于公用数据网上以分组方式工作的 DTE 和 DCE 之间的接口标准。X.25 规范对应 OSI 三层，X.25 的第三层描述了分组的格式及分组交换的过程。X.25 的第二层由 LAPB（Link Access Procedure Balanced，链路访问过程平衡）实现，它定义了用于 DTE/DCE 连接的帧格式。X.25 的第一层定义了电气和物理端口特性。

X.25 网络设备分为数据终端设备（DTE）、数据电路终端设备（DCE）及分组交换设备（PSE），如图 6.2 所示。DTE 是 X.25 的末端系统，如终端、计算机或网络主机，一般位于用户端，Cisco 路由器就是 DTE 设备。DCE 设备是专用通信设备，如调制解调器和分组交换机。PSE 是公共网络的主干交换机。

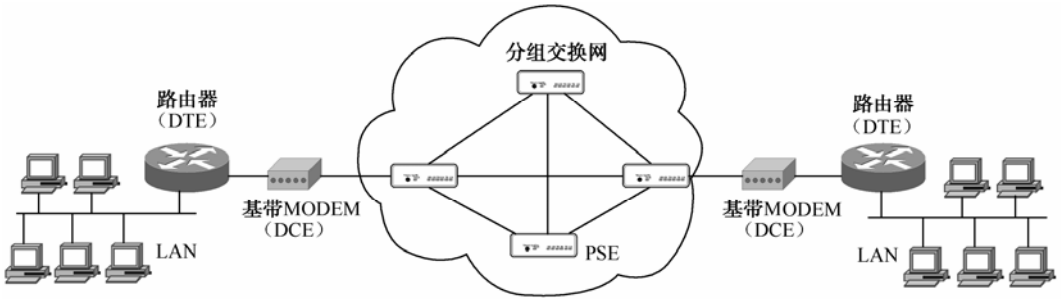


图 6.2　X.25 网络

3．CHINAPAC简介

中国公用分组交换网（CHINAPAC）是由原邮电部组建的以 X.25 网为基础、可以满足不同传输速率、不同型号 DTE 及 LAN 之间通信和资源共享的计算机通信网。该网于 1993 年开通运行，骨干网覆盖了全国所有省会城市，各省还有省网、市网，在北京、上海都有国际出入口与国际数据网互连。它是国内分布最广、使用环境最好的数据通信网。

6.2.4　帧中继（Frame Relay）

1．帧中继技术简介

帧中继是一种高性能的 WAN 协议，它运行在 OSI 参考模型的物理层和数据链路层。它是一种数据包交换技术，是 X.25 的简化版本。它省略了 X.25 的一些强健功能，如提供窗口技术和数据重发技术，而是依靠高层协议提供纠错功能，这是因为帧中继工作在更好的 WAN 设备上，这些设备比 X.25 的 WAN 设备具有更可靠的连接服务和更高的可靠性，它严格地对应于 OSI 参考模型的物理层和数据链路层，而 X.25 还提供第三层的服务，所以帧中继比 X.25 具有更高的性能和更有效的传输效率。

帧中继网络如图 6.3 所示。帧中继广域网的设备分为数据终端设备（DTE）和数据电路终端设备（DCE），Cisco 路由器作为 DTE 设备。

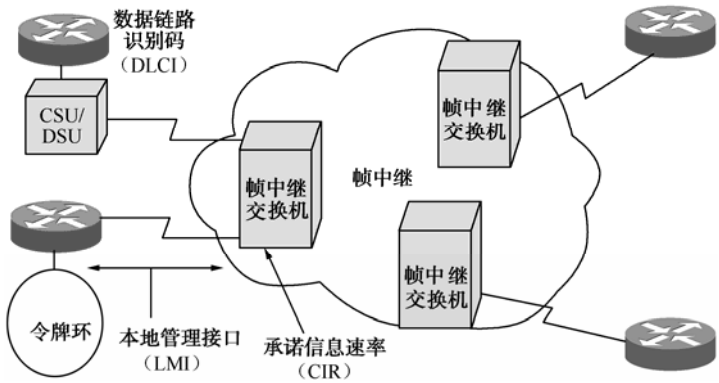


图 6.3　帧中继网络

帧中继技术提供面向连接的数据链路层的通信，在每对设备之间都存在一条定义好的通信链路，并且该链路有一个数据链路识别码。这种服务通过帧中继虚电路实现，每个帧中继虚电路都以数据链路识别码（DLCI）标志自己。DLCI 的值一般由帧中继服务提供商指定。帧中继既支持由服务提供商预先设置的永久虚电路（PVC），也支持动态虚电路（SVC）。

帧中继本地管理接口（LMI）是对基本的帧中继标准的扩展。它是路由器和帧中继交换机之间的信令标准，提供帧中继管理机制。它提供了许多管理复杂互连网络的特性，其中包括全局寻址、虚电路状态消息和多目的发送等功能。

2．帧中继的常见应用

帧中继的常见应用简介如下：

（1）局域网的互连。由于帧中继具有支持不同数据速率的能力，使其非常适于处理局域网到局域网的突发数据流量。传统的局域网互连，每加一条端到端线路，就要在用户的路由器上增加一个端口。基于帧中继的局域网互连，只要局域网内的每个用户至网络间有一条带宽足够的线路，则既不用增加物理线路也不占用物理端口，就可增加端到端线路，而不致对用户性能产生影响。

（2）语音传输。帧中继不仅适用于对时延不敏感的局域网的应用，还可以进行对时延要求较高的低档语音的应用。

（3）文件传输。帧中继既可保证用户所需的带宽，又有令人较满意的传输时延，非常适合大流量文件的传输。

6.2.5　数字数据网（DDN）

1．什么是DDN

DDN 的全名是数字数据网（Digital Data Network），它是利用数字信道提供永久或半永久性连接、传输数字信号的数字传输网络。它采用的传输介质有光纤、数字微波、卫星信道以及用户端可用的普通电缆和双绞线。它包含了数据通信、数字通信、数字传输、数字交叉连接、计算机带宽管理等技术，可根据用户的需要，在短时间内接通所需的带宽线路，为客户建立自己的专业数据网提供条件。

2．DDN的特点

（1）DDN 专线是实现端到端的数字连接的同步数字传输信道，其传输质量直接取决于光纤传输系统，误码率可达 10^{-11}，同时数字专线电路便于复用和加密，传输质量高。

（2）DDN 是一种全透明的数据传输网，支持各种协议和规程，可用于传输数据、图像、话音等多种业务。

（3）与固定物理连接的电话专线相比，DDN 专线是临时的半固定连接网络，用户所需的数据传输速率和信道带宽可根据需要灵活设置。

（4）DDN 将检错纠错等功能放到智能化程度较高的终端完成，简化了网络运行管理和控制的内容；同时，DDN 节点之间的中继和电路都有备份，当电路发生故障时可自动迂回，保障网络的正常工作。

（5）DDN 设置了网络管理中心，可随时监控网络运行状态，及时发现故障，并采取相应的措施，保障网络的正常运行；同时还可以方便地建立用户之间所需要的专线电路，拆除电路、调度电路也方便、快捷。

（6）与 X.25 网相比，DDN 能为用户提供高质量的数字数据传输信道。X.25 提供的是具

有交换功能的传输信道，分组网的用户在需要时就能进行相互间的通信。DDN 为用户提供的是点到点的专用的、固定的数字数据信道。对于通信业务比较繁忙、传输质量要求较高且通信对象相对集中的用户来讲，适于采用 DDN。

3．DDN的组成

DDN 由网络设备、连接电路和网络拓扑组成。

（1）网络设备。包括网络节点、网络接入单元和网络设备。网络节点是 DDN 的基本组成单位，节点间通过光纤连接。网络接入单元可以是数据服务单元、信道服务单元。

（2）连接电路。连接电路包括从用户设备的网络接入单元到节点间的用户线和节点间的中继设备。

（3）网络拓扑。网络拓扑指节点间的相互连接方式。DDN 节点使用光纤相互连接，构成网状拓扑结构。

4．用户终端接入DDN的方式

用户终端接入 DDN 的方式主要包括：

（1）通过 MODEM 接入 DDN。当用户远离 DDN 节点时，适合采用这种接入方式。

（2）通过数据终端设备接入 DDN。数据终端设备是 DDN 节点的配套设备，用于延伸 DDN 专线至用户终端。

（3）通过用户集中设备接入 DDN。用户集中设备的作用是将多用户数据集中起来传输。用户集中设备实际上是一种复用器，当用户需要租用多条 64kbps 的信道时，采用这种方式可节省用户线路费用。

（4）通过路由器接入 DDN 专线。局域网用户可通过路由器入网，接入速率可达 2Mbps。

（5）通过模拟电路接入 DDN。适用于电话机、传真机和用户交换机经模拟电路传输后直接接入 DDN 的音频接口。

6.3 网络互连技术

6.3.1 网络互连技术概述

网络互连是指将不同的网络连接起来，以构成更大规模的网络系统，实现网络间的数据通信和资源共享。

1．网络互连的必要性

（1）ISO/OSI 虽然问世多年，但在实际运行中依然存在大量非 OSI 的网络，而且各种现有的特定网络并不一定都采用 OSI 七层模型。

（2）OSI 采用了通信子网和现有的多种网络产品，它本身就决定了各种类型的通信子网一直共存下去。

（3）网络互连可以改善网络性能：提高系统的可靠性、改进系统的性能、增加系统保密性、建网方便、增加地理覆盖范围。

随着商业需求的推动，特别是 Internet 的深入人心，网络互连技术成为实现如 Internet 这样的大规模通信和资源共享的关键技术。

2．网络互连的目的

由于不同的网络间可能存在各种差异，因此对网络互连有如下要求：

（1）在网络之间提供一条链路，至少需要一条物理和链路控制的链路。

（2）提供不同网络间的路由选择和数据传送。

（3）提供各用户使用网络的记录和保持状态信息。

（4）在网络互连时，应尽量避免由于互连而降低网络的通信性能。

（5）不修改互连在一起的各网络原有的结构和协议。这就要求网络互连设备应能进行协议转换，协调各个网络的不同性能。

当源网络发送分组到目的网络要跨越一个或多个外部网络时，这些性能差异会使得数据包在穿过不同网络时会产生很多问题。网络互连的目的就在于提供不依赖于原来各个网络特性的互连网络服务。

3．网络互连的类型

网络互连可分为 LAN-LAN、LAN-WAN、LAN-WAN-LAN、WAN-WAN 四种类型。

（1）LAN-LAN。LAN-LAN 又分为同种 LAN-LAN 和异种 LAN-LAN。常用设备有中继器和网桥。LAN-LAN 如图 6.4 所示。

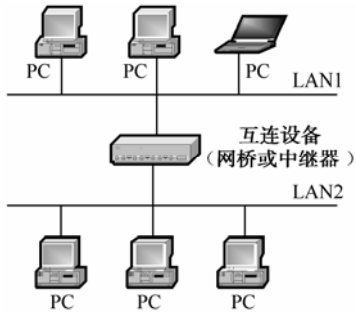


图 6.4　LAN-LAN

（2）LAN-WAN。用来连接的设备是路由器或网关，如图 6.5 所示。

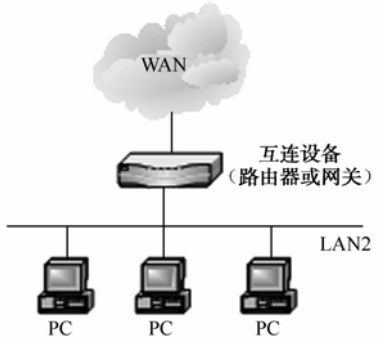


图 6.5　LAN-WAN

（3）LAN-WAN-LAN。是将两个分布在不同地理位置的 LAN 通过 WAN 实现互连，连接设备主要有路由器和网关，如图 6.6 所示。

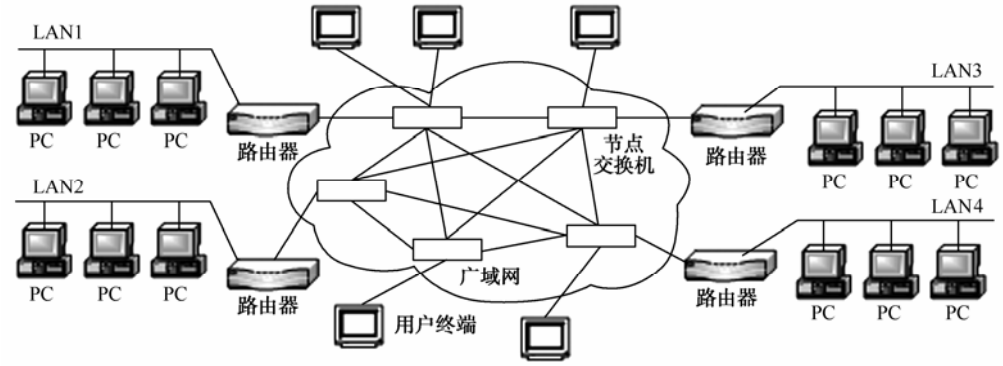


图 6.6　LAN-WAN-LAN

（4）WAN-WAN。通过路由器和网关将两个或多个广域网互连起来，可以使分别连入各个广域网的主机资源能够实现共享，如图 6.7 所示。

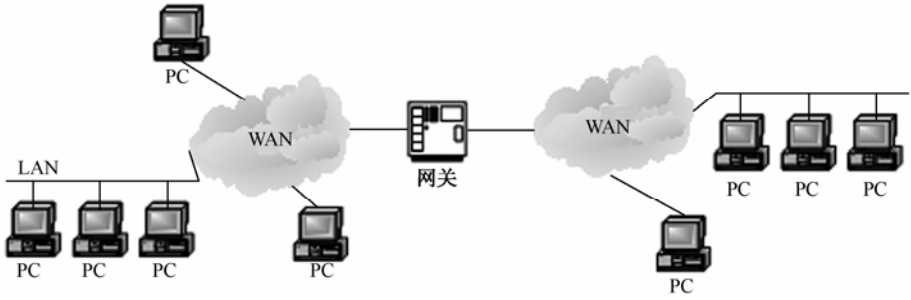


图 6.7　WAN-WAN

6.3.2　IP地址

IP 地址是按照 IP 协议规定的格式，为每一个正式接入 Internet 的主机所分配的、供全世界标志的惟一通信地址。目前，全球广泛应用的 IP 协议是 4.0 版本，记为 IPv4，因而 IP 地址又称为 IPv4 地址，本节提及的 IP 地址除特殊说明外均指 IPv4 地址。

1．IP地址结构和编址方案

IP 地址用 32 位二进制编址，分为 4 个 8 位组，由网络号 netid 和主机号 hostid 两部分构成。网络号确定了该台主机所在的物理网络，它的分配必须全球统一；主机号确定了在某一物理网络上的一台主机，它可由本地分配，不需全球一致。

根据网络规模，IP 地址分为 A～E 五类。A、B、C 类称为基本类，用于主机地址，下面将做详细介绍；D 类用于组播；E 类保留不用。IP 地址编码方案如图 6.8 所示。

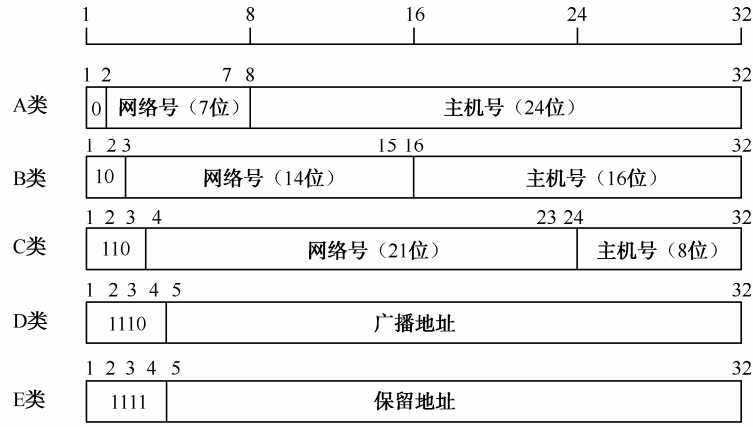


图 6.8　IP 地址编址方案

（1）A 类地址。在 IP 地址的 4 段号码中，第一段号码为网络号码，剩下的 3 段号码为本地计算机的号码。如果用二进制表示 IP 地址，A 类 IP 地址就由 1 字节的网络地址和 3 字节的主机地址组成，网络地址的最高位必须是“0”。A 类 IP 地址中的网络标志长度为 7 位，主机标志长度为 24 位。A 类网络地址数量较少，一般分配给少数规模达 1700 万台主机的大型网络。

（2）B 类地址。在 IP 地址的 4 段号码中，前 2 段号码为网络号码，B 类 IP 地址就由 2 字节的网络地址和 2 字节的主机地址组成，网络地址的最高位必须是“10”。B 类 IP 地址中的网络标志长度为 14 位，主机标志长度为 16 位。B 类网络地址适用于中等规模的网络，每个网络所能容纳的计算机数为 6 万多台。

（3）C 类地址。在 IP 地址的 4 段号码中，前 3 段号码为网络号码，剩下的 1 段号码为本地计算机的号码。如果用二进制表示 IP 地址，C 类 IP 地址就由 3 字节的网络地址和 1 字节的主机地址组成，网络地址的最高位必须是“110”。C 类 IP 地址中的网络标志长度为 21 位，主机标志长度为 8 位。C 类网络地址数量较多，适用于小规模的局域网络，每个网络能够有效使用的最多计算机数为 254 台。例如，某大学现有 64 个 C 类地址，可包含有效使用的计算机总数为 254×64=16256 台。

三类 IP 地址空间分布为：A 类网络共有 126 个，B 类网络共有 16000 多个，C 类网络共有 200 多万个。三种主要 IP 地址包含的网络数和主机数如表 6.1 所示。

表 6.1　三种主要 IP 地址包含的网络数和主机数

地址类	前缀二进制位数	后缀二进制位数	网络最大数	网络中最大主机数
A	7	24	$126(2^7-2)$	$16777214(2^{24}-2)$
B	14	16	$16382(2^{14}-2)$	$65534(2^{16}-2)$
C	21	8	$2097152(2^{21}-2)$	$254((2^8-2)$

2．IP地址表示方式

IP 地址是 32 位二进制数，不便于用户输入、读数和记忆，因此用一种“点分十进制”数来表示，其中每 8 位一组用十进制表示，并利用点号分割各部分，每组值的范围为 0～255，IP 地址用此种方法表示的范围为 0.0.0.0～255.255.255.255。根据上述规则，IP 地址范围及说明如表 6.2 所示。

表 6.2　IP 地址范围及说明

地址类	网络标志范围	特殊 IP 说明
A	0~127	0.0.0.0 保留，作为本机 0.x.x.x 保留，指定本网中的某个主机 10.x.x.x，供私人使用的保留地址 127.x.x.x 保留用于回送，在本地机器上进行测试和实现进程间通信。发送到 127 的分组永远不会出现在任何网络上
B	128~191	172.16.x.x～172.31.x.x，供私人使用的保留地址
C	192~223	192.168.0.x～192.168.255.x，供私人使用的保留地址，常用于局域网中
D	224~239	用于广播传送至多个目的地址
E	240~255	保留地址 255.255.255.255 用于对本地网上的所有主机进行广播，地址类型为有限广播
注：① 主机号全为 0 用于标志一个网络的地址，如 106.0.0.0 指明网络号为 106 的一个 A 类网络 ② 主机号全为 1 用于在特定网上广播，地址类型为直接广播，如 106.1.1.1 用于在 106 段的网络上向所有主机广播		

6.3.3　子网划分

对于一些小规模的网络和企业、机构内部网络，即使使用一个 C 类网络号，但仍然是一种浪费，因而在实际应用中，需要对 IP 地址中的主机号部分进行再次划分，将其划分成子网号和主机号两部分，从而把一个包含大量主机的网络划分成许多小的网络，每个小网络就是一个子网。每个子网都是一个独立的逻辑网络，单独寻址和管理，而对外部它们组成一个单一网络，共享某一 IP 地址，屏蔽内部子网的划分细节。

1．子网和主机

图 6.9 显示出 B 类地址子网地址划分。在此例中，B 类地址的主机地址共 16 位，取主机地址的高 7 位作为子网地址，低 9 位作为每个子网的主机号。

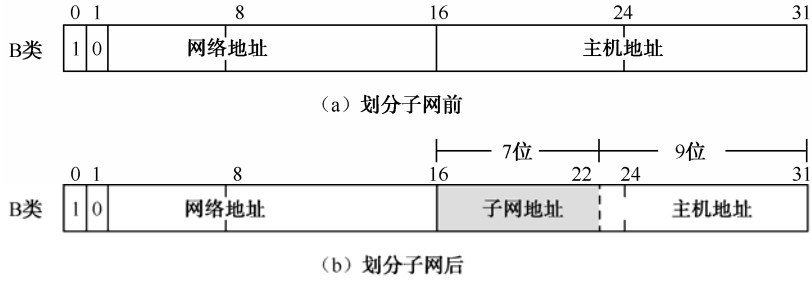


图 6.9　B 类地址子网划分

假定原来的网络地址为 128.10.0.0，划分子网后，128.10.2.0 表示第 1 个子网，128.10.4.0 表示第 2 个子网，128.10.6.0 表示第 3 个子网……

在这个方案中，实际最多可以有 $2^7-2=126$ 个子网（不含全 0 和全 1 的子网，因为路由协议不支持全 0 或全 1 的子网掩码，全 0 和全 1 的网段都不能使用）。每个子网最多可以有 $2^9-2=510$ 台主机（不含全 0 和全 1 的主机）。

子网地址的位数没有限制（但显然不能是 1 位，其实 1 位的子网地址相当于并未划分子

网，主机地址也不能只保留 1 位），可由网络管理人员根据所需子网个数和子网中主机数目确定。

2．子网掩码

在数据的传输中，路由器必须从 IP 数据报的目的 IP 地址中分离出网络地址，才能知道下一站的位置。为了分离网络地址，就要使用子网掩码。

子网掩码为 32 位二进制数值，分别对应 IP 地址的 32 位二进制数值。对应 IP 地址中的网络号部分在子网掩码中用“1”表示，对应 IP 地址中的主机号部分在子网掩码中用“0”表示。由此，A、B、C 三类地址对应的子网掩码如下：

（1）A 类地址的子网掩码为 255.0.0.0。

（2）B 类地址的子网掩码为 255.255.0.0。

（3）C 类地址的子网掩码为 255.255.255.0。

划分子网后，将 IP 地址的子网掩码中对应子网地址的位设置为 1，就形成了子网掩码，又称子网屏蔽码，它可从 IP 地址中分离出子网地址，供路由器选择路由。换句话说，子网掩码用来确定如何划分子网。例如，若将 B 类 IP 地址中主机地址的高 7 位设为子网地址，则其子网掩码为 255.255.254.0。

在选择路由时，用子网掩码与目的 IP 地址按二进制位做“与”运算，就可保留 IP 地址中的网络地址部分，而屏蔽主机地址部分。同理，将掩码的反码与 IP 地址做逻辑“与”操作，可得到其主机地址。例如获取网络地址：

	10000000 00010101 00000011 00001100	（IP **地址** 128.21.3.12）
“与”运算	11111111 11111111 00000000 00000000	（**网络掩码** 255.255.0.0）
结果	10000000 00010101 00000000 00000000	（**网络地址** 128.21.0.0）

例如，一个 C 类网络地址 192.168.23.0，利用掩码 255.255.255.192 可将该网络划分为 4 个子网：192.168.23.0、192.168.23.64、192.168.23.128、192.168.23.192，其中有效使用的为 2 个子网（192.168.23.64 和 192.168.23.128）。如果网内一个 IP 地址是 192.168.23.186，则通过掩码可知，它的子网地址为 192.168.23.128，主机地址为 0.0.0.58。

由此可见，子网掩码不仅可以将一个网段划分为多个子网段，便于网络管理，还有利于网络设备尽快地区分本网段地址和非本网段的地址。

下面用一个例子说明子网掩码的这一作用和其应用过程。如图 6.10 所示，主机 A 与主机 B 交互信息。在 IP 协议中，主机或路由器的每个网络接口都分配有 IP 地址和对应的掩码。

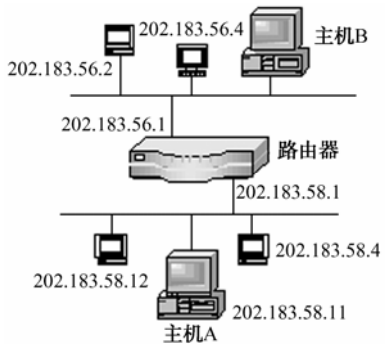


图 6.10　子网掩码应用实例

（1）主机 A 的 IP 地址：202.183.58.11。

子网掩码：255.255.255.0。

路由地址：202.183.58.1。

（2）主机 B 的 IP 地址：202.183.56.5。

子网掩码：255.255.255.0。

路由地址：202.183.56.1。

路由器从端口 202.183.58.1 接收到主机 A 发往主机 B 的 IP 数据报文后：

（1）用端口地址 202.183.58.1 与子网掩码地址 255.255.255.0 进行“逻辑与”，得到端口网段地址 202.183.58.0。

（2）将目的地址 202.183.56.5 与子网掩码地址 255.255.255.0 进行“逻辑与”，得目的网段地址 202.183.56.0。

（3）将结果 202.183.56.0 与端口网段地址 202.183.58.0 比较，如果相同，则认为是本网段的，不予转发。如果不相同，则将该 IP 报文转发到端口 202.183.56.1 所对应的网段。

6.3.4 网络互连设备

由于网络间存在不同的差异，所以就需要用不同的网络互连设备将各个网络连接起来。根据网络互连设备工作的层次及其所支持的协议，可以将网间设备分为中继器、网桥（或二层交换机）、路由器（或三层交换机）和网关，如图 6.11 所示。

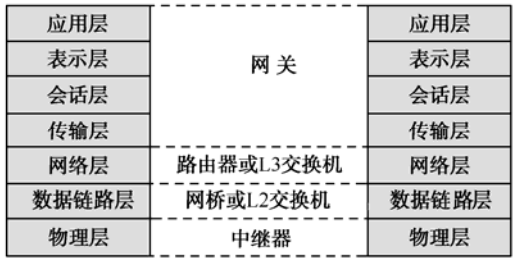


图 6.11 网络互连设备所处的层次

1．物理层互连设备

物理层：用于不同地理范围内的网段的互连。通过互连，在不同的通信介质中传送比特流，要求连接的各网络的数据传输率和链路协议必须相同。

设备：中继器。工作在物理层的网间设备主要是中继器，用于扩展网络传输的长度，实现两个相同的局域网段间的电气连接。它仅仅是将比特流从一个物理网段复制到另一个物理网段，而与网络所采用的网络协议（如 TCP/IP、IPX/SPX、NETBIOS 等）无关。

中继器具有如下特性：

（1）中继器仅作用于物理层。

（2）只具有简单的放大、再生物理信号的功能。

（3）由于中继器工作在物理层，在网络之间实现的是物理层连接，因此中继器只能连接相同的局域网。

（4）中继器可以连接相同或不同传输介质的同类局域网。

（5）中继器将多个独立的物理网连接起来，组成一个大的物理网络。

（6）由于中继器在物理层实现互连，所以它对物理层以上各层协议完全透明，也就是说，

中继器支持数据链路及其以上各层的所有协议。

使用中继器时应注意两点：一是不能形成环路；二是考虑到网络的传输延迟和负载情况，不能无限制地连接中继器。

2．数据链路层互连设备

数据链路层：用于互连两个或多个同一类型的局域网，传输帧。

设备：网桥（或二层交换机）。网桥可以连接两个或多个网段。如果信息不是发向网桥所连接的网段，则网桥可以过滤掉该信息。

1）网桥的工作原理

参见 2.5.1 节的内容。

2）网桥带来的问题

（1）广播风暴。网桥要实现帧转发功能，必须保存一张“端口—节点地址表”。随着网络规模的扩大与用户节点数的增加，实际的“端口—节点地址表”的存储能力有限，会不断出现“端口—节点地址表”中没有的节点地址信息。当带有这一类目的地址的数据帧出现时，网桥就将该数据帧向除输入端口之外的其他所有端口中广播出去。这种盲目发送数据帧的做法，造成“广播风暴”。

（2）增加网络时延。网桥在互连不同的局域网时，需要对接收到的帧进行重新格式化，以适合另一个局域网 MAC 子层的要求，还要重新对新的帧进行差错校验计算，这就造成了时延的增加。

（3）帧丢失。当网络上的负荷很重时，网桥会因为缓存的存储空间不够而发生溢出，造成帧丢失。

3．网络层互连设备

网络层：主要用于广域网的互连。网络层互连解决路由选择、阻塞控制、差错处理、分段等问题。

设备：路由器（或三层交换机）。工作在网络层的网间设备主要是路由器。路由器提供各种网络间的网络层接口。路由器是主动的、智能的网络节点，它们参与网络管理，提供网间数据的路由选择，并对网络的资源进行动态控制等。路由器是依赖于协议的，它必须对某一种协议提供支持，如 IP、IPX 等。

1）路由器工作原理

参见 2.6.2 节的内容。

2）路由器的功能

（1）路由选择。路由器中有一个路由表，当连接的一个网络上的数据分组到达路由器后，路由器根据数据分组中的目的地址，参照路由表，以最佳路径把分组转发出去。路由器还有路由表的维护能力，可根据网络拓扑结构的变化，自动调节路由表。

（2）协议转换。路由器可对网络层和以下各层进行协议转换。

（3）实现网络层的一些功能。因为不同网络的分组大小可能不同，所以路由器有必要对数据包进行分段、组装，调整分组大小，使之适合于下一个网络对分组的要求。

（4）网络管理与安全。路由器是多个网络的交汇点，网间的信息流都要经过路由器，在路由器上可以进行信息流的监控和管理。它还可以进行地址过滤，阻止错误的数据进入，起到“防火墙”的作用。

（5）多协议路由选择。路由器是与协议有关的设备，不同的路由器支持不同的网络层协议。多协议路由器支持多种协议，能为不同类型的协议建立和维护不同的路由表，连接运作

不同协议的网络。

3）路由器的不足

路由器的配置和管理技术复杂，成本昂贵，而且它的接入增加了数据传输的时间延迟，在一定程度上降低了网络的性能。

4）路由器与第三层交换机的比较

第三层交换机是将局域网交换机的设计思想应用在路由器的设计中产生的。随着 Internet 的广泛应用，第三层交换技术已成为一项重要技术。第三层交换机又称路由交换机或交换式路由器，虽然这些名称不同，但它们所表达的内容基本上是相同的。

传统的路由器通过软件来实现路由选择功能，而第三层交换的路由器通过专用集成电路（ASIC）芯片来实现路由选择功能。第三层交换设备的数据包处理时间将由传统路由器的几千微秒量级减少到几十微秒量级，甚至更短，因此大大缩短了数据包在交换设备中的传输延迟时间。

4．高层互连设备

高层：用于在网络层以上的高层之间进行不同协议的转换，它也是最复杂的。

设备：网关。工作在第三层以上的网络互连设备称为网关，它的作用是连接两个或多个不同的网络，使之能相互通信。这种“不同”常常是物理网络和高层协议都不一样，网关必须提供不同网络间协议的相互转换。最常见的如将某一特定种类的局域网或广域网与某个专用的网络体系结构相互连接起来。

1）网关的工作原理

网关用于类型不同且差别较大的网络系统间的互连，主要用于不同体系结构的网络或者局域网与主机系统的连接。在互连设备中，它最为复杂，一般只能进行一对一的转换，或是少数几种特定应用协议的转换。它的概念模型如图 6.12（a）所示。

图 6.10（b）给出了网关的工作原理示意图。如果一个 NetWare 节点要与 TCP/IP 的主机通信，因为 NetWare 和 TCP/IP 协议是不同的，所以局域网中的 NetWare 节点不能直接访问。它们之间的通信必须由网关来完成。网关的作用是为 NetWare 产生的报文加上必要的控制信息，将它转换成 TCP/IP 主机支持的报文格式。当需要反方向通信时，网关同样要完成 TCP/IP 报文格式到 NetWare 报文格式的转换。

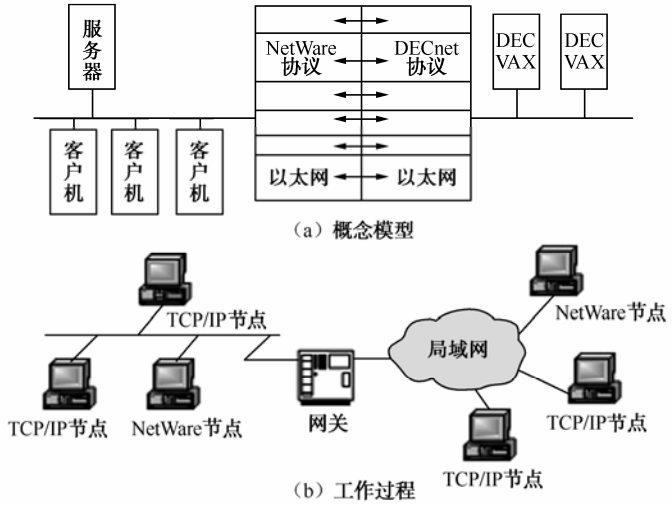


图 6.12　网关的工作原理示意图

2）网关的主要变换项目

网关的主要变换项目包括信息格式变换、地址变换、协议变换等。

（1）格式变换。格式变换是将信息的最大长度、文字代码、数据的表现形式等变换成适用于对方网络的格式。

（2）地址变换。由于每个网络的地址构造不同，因而需要变换成对方网络所需要的地址格式。

（3）协议变换。把各层使用的控制信息变换成对方网络所需的控制信息，由此可以进行信息的分割/组合，数据流量控制、错误检测等。

3）网关的分类

网关按其功能可以分为三种类型：协议网关、应用网关和安全网关。

（1）协议网关。协议网关通常在使用不同协议的网络间做协议转换工作，这是网关最常见的功能。协议转换必须在数据链路层以上的所有协议层都运行，而且要对节点上使用这些协议层的进程透明。因为协议转换必须考虑两个协议之间特定的相似性和差异性，所以协议网关的功能十分复杂。

（2）应用网关。应用网关是在应用层连接两部分应用程序的网关，是在不同数据格式间翻译数据的系统。这类网关一般只适合于某种特定的应用系统的协议转换。

（3）安全网关。安全网关就是防火墙。与网桥一样，网关可以是本地的，也可以是远程的。另外，一个网关还可以由两个半网关构成。目前，网关已成为网络上每个用户都能访问大型主机的通用工具。

6.4 交换机的一般配置

6.4.1 交换机的配置基础

1．Cisco IOS简介

Cisco Catalyst 系列交换机所使用的操作系统是 IOS（Internetwork Operation System）或 COS（Catalyst Operation System），而 IOS 使用最为广泛。IOS 不仅作为 Cisco Catalyst 系列交换机的操作系统，也是 Cisco 系列路由器的操作系统。使用 IOS 的路由器和交换机具有相同的内核和操作命令。本节将以采用 Cisco IOS 的交换机为例来介绍交换机的基本配置。

2．交换机的配置方式

1）通过 Console 端口配置

Console 端口是交换机和路由器等网络设备的基本端口，它是用户对一台新交换机和路由器进行配置时必须使用的接口。连接 Console 端口的线缆是反转线，线的一端是 RJ-45 插头和 8 芯线；另一端的线序完全相反，并且插头可能是 RJ-45，也可能是 DB-9 或 DB-25。通过 Console 端口对设备进行访问是最直接和最有效的控制设备的方法，也是在配置网络设备时使用最多的一种方式。

2）通过 Telnet 访问

在实际的网络运营中，如果网络设备设置了正确的管理 IP 地址和远程登录密码，就可以通过 Telnet 远程登录方式来配置交换机。以 Cisco 设备为例，它把每一个远程登录用户作为一个 VTY（Vitrual Type Terminal，虚拟终端），交换机支持 16 个 VTY，为 VTY 0～VTY 15，

这也就意味着同时可有 16 个用户通过 Telnet 方式访问交换机。也可以先利用超级终端程序登录到一台交换机或路由器后，再从其他交换机或路由器上执行 Telnet 来访问远程的交换机。

3）通过浏览器访问

现在，很多网络设备都支持通过浏览器访问，通过图形化的操作方式，简化用户的操作。对于 Cisco 交换机，需要先进行相应配置，在交换机的全局配置模式下，输入 ip http server 命令，让交换机支持浏览器访问，然后就可以通过浏览器软件访问交换机。不过，在运营的网络上，为保证安全，一般不通过浏览器软件访问。

4）通过网管软件来访问

大部分网络设备都支持 SNMP（简单网络管理协议），通过对网络设备配置相应的 SNMP 参数，在网管工作站上运行网管软件就可以对这些设备进行配置和检测。

3．Cisco IOS的访问模式

Cisco IOS 提供三种基本的访问模式：用户 EXEC 模式、特权 EXEC 模式和配置模式。在任何一种模式下，键入“?”，均可得到该模式下允许执行的命令帮助。

1）用户 EXEC 模式（User EXEC）

用户 EXEC 模式是 IOS 启动时的默认模式，当用户通过控制台端口或 Telnet 连接并登录到交换机时，此时的模式就处在用户 EXEC 模式下。该模式提供有限的访问权限，允许执行一些非破坏性的操作，允许查看配置参数，测试连通性等，但不能对配置做任何改动。用户 EXEC 模式下的提示符为“>”，如 switch>或 router>。

2）特权 EXEC 模式（Privileged EXEC）

特权 EXEC 模式也称使能（Enable）模式，可对交换机或路由器进行更多的操作，使用的命令集比用户模式多，可对交换机和路由器进行更高级的测试，如使用 debug 命令。在用户 EXEC 模式下通过 enable 命令进入特权 EXEC 模式。特权 EXEC 模式的提示符为“#”。交换机和路由器的特权 EXEC 模式命令的默认状态行分别为 switch#和 router#。

3）配置模式（Configuration）

配置模式是交换机和路由器的最高操作模式，可以设置交换机和路由器上运行的硬件和软件的相关参数，配置各接口、VLAN、路由协议，设置用户和访问密码等。

配置模式又分为全局配置模式和几种子模式，子模式有接口配置模式、线路配置模式、VLAN 数据库配置模式和路由协议配置模式等。

各种模式的提示符以及各种模式之间转换的命令如图 6.13 所示。

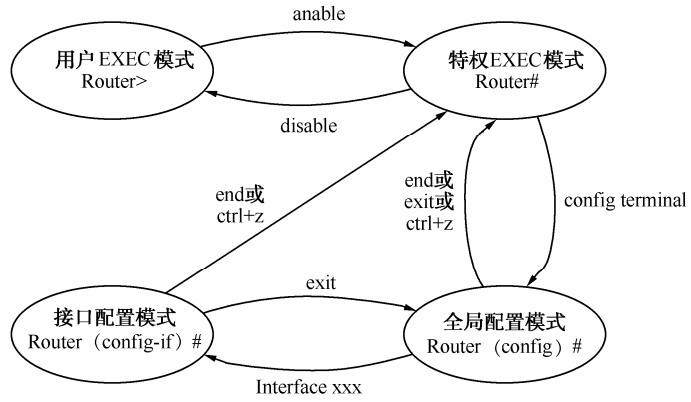


图 6.13　各种模式的提示符以及各种模式之间转换的命令

6.4.2 交换机的基本配置内容

1．交换机的加电与配置向导

给交换机加电后，交换机就开始启动。首先运行自检程序，然后加载 flash 中的 IOS。IOS 加载完后，在 NVRAM 中寻找交换机的配置文件，将其装入内存（RAM）中运行。当软、硬件初始化完成后，出现下面的系统配置对话：

```
        --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
```

对于初次使用的交换机，在启动时会询问是否进入初始配置对话，可以选择“yes”，进入配置向导。在任何时刻，都可按 Ctrl+C 组合键来终止配置。也可以选择“no”，跳过系统配置向导。

2．配置主机名和密码

配置主机名和特权密码要在全局配置模式下通过 hostname 命令和 enable password 命令来实现，其命令格式如下：

```
hostname hostname
enable password password
```

配置 vty 线路和 Console 端口的登录密码是在相应的线路配置模式下使用如下命令：

```
password password
login
```

例：配置交换机的主机名为 Switch2950，进入特权 EXEC 模式的密码为 cisco-en，vty0~4 条线路的登录密码为 cisco-vty，Console 的登录密码为 cisco-con。

```
switch>enable                                          //进入特权 EXEC 模式
switch#configure terminal                              //进入全局配置模式
Enter configuration commands, one per line.   End with CNTL/Z.
switch(config)#hostname Switch2950                     //配置交换机的主机名为 Switch2950
Switch2950(config)#enable password cisco-en            //配置特权访问密码为 cisco-en
Switch2950(config)#line con 0                          //进入 con 线路配置模式
Switch2950(config-line)#password cisco-con             //设置置 console 端口访问密码为 cisco-con
Switch2950(config-line)#login                          //允许密码验证
Switch2950(config-line)#line vty 0 15                  //进入 vty0~15 条线路配置
Switch2950(config-line)#password cisco-vty             //设置 vty 端口访问密码为 cisco-vty
Switch2950(config-line)#login                          //允许密码验证
Switch2950(config-line)# end                           //结束配置，回到特权 EXEC 模式
Switch2950#
```

3．指定交换机的管理IP地址和默认网关

为使交换机能被 Telnet 和其他 TCP/IP 应用程序访问，需要给交换机指定 IP 地址和默认网关。在默认情况下，VLAN1 是管理 VLAN，在基于交换的网络中，所有网络设备都应该属于同一个管理 VLAN。这样，仅用一台管理工作站就可以访问、配置和管理所有网络设备。

配置 IP 地址的命令格式为：

```
ip address address subnet-mask
```

配置默认网关的命令格式为：

```
ip default-gateway gateway address
```

下面的例子显示了如何为 Catalyst 2950 交换机设置管理 IP 地址和默认网关。

例：设置交换机的管理 IP 地址和默认网关。

```
Switch2950#configure terminal                                    //进入全局配置模式
Switch2950 (config)#interface vlan1                              //进入 vlan1 接口
Switch2950 (config-if)#ip address 192.168.10.1 255.255.255.0    //设置交换机的管理 IP 地址
Switch2950 (config)#ip default-gateway 192.168.10.254            //设置交换机的默认网关
Switch2950 (config)#^Z                          //Ctrl+Z 结束配置，回到特权 EXEC 模式
Switch2950#
```

4．查看交换机信息

（1）查看 IOS 版本信息。可以用 show version 命令来验证 IOS 版本和配置寄存器的设置。在该输出中还可以看到交换机的其他信息，如 IOS 系统映像文件名、交换机型号、序列号、内存大小、端口数量和类型。

（2）显示交换机的配置信息。使用 show running-config 命令来显示交换机的当前运行配置。用 show startup-config 命令来显示保存在 NVRAM 中的启动配置。

（3）查看交换机端口信息。使用 show interface 命令可以看到端口信息，其用法为：

```
show interface type mode/port
```

（4）查看 VLAN 信息。在默认情况下，交换机的所有端口都属于 VLAN1，VLAN1 作为默认的管理 VLAN。使用 show vlan 命令可以显示交换机中所定义的 VLAN 的相关信息。

（5）查看闪存目录。使用 dir flash 命令可以查看闪存目录（flash directory）里包含的文件信息。在闪存目录中的文件一般有 IOS 映像文件（以.bin 结尾）、VLAN 数据库文件（vlan.dat）、配置文件（config.text）、一个名为 env_vars 的文件以及一个 html 子目录。

5．管理MAC地址表

交换机通过检查在端口上接收到的帧的源地址就可以学习到连接在该端口的 PC 或工作站的 MAC 地址。这些地址被记录在 MAC 地址表中。如果帧的目的 MAC 地址已经记录在该表中，则该帧就能转发到正确的接口上。

（1）检查交换机的 MAC 地址表。

```
show mac-address-table
```

（2）清除 MAC 地址表。

```
clear mac-address-table
```

（3）配置静态 MAC 地址。可以通过配置静态 MAC 地址将一个 MAC 地址永久分配给一个端口，交换机不会自动地将该 MAC 地址过期。为了设置交换机接口的静态 MAC 地址条目，在全局配置模式下使用如下命令：

```
mac-address-table static mac-address-of-host vlan vlan-id interface interface-id
```

要把该条目删除，可以用 no 形式的命令。

6．恢复交换机的默认配置

为了确保新的配置完全覆盖当前存在的配置，必须恢复交换机的默认配置。步骤如下：

（1）删除闪存目录中的 VLAN 数据库文件，从而删除现有的 VLAN 信息。

（2）删除配置备份文件 startup-config。

（3）重新启动交换机。

例：恢复 Switch2950 的默认配置。

```
Switch2950#delete flash:vlan.dat
Delete filename[vlan.dat]?                          //回车
Delete flash:vlan.dat?[confirm]                     //回车
Switch2950#erase startup-config
……
Switch2950#reload
```

6.4.3　配置交换机端口

1．端口选择

使用 IOS 的交换机，交换机的端口通常也称为接口（Interface），它由端口的类型、模块号和端口号来进行标志，端口选择的命令可在全局配置模式下使用，也可在接口配置模式下使用。

端口选择命令为：

```
interface type slot/port                            //选择某一个端口
interface range type slot/{first port} - {last port}  //选择一组端口
```

当使用 interface range 命令时，有如下的规则：

```
fastethernet slot/{first port} - {last port}        //模块为 0
gigabitethernet slot/{first port} - {last port}     //模块为 0
```

端口号之间需要加入空格，如 interface range fastethernet 0/1-5 是有效的，而 interface range fastethernet 0/1-5 是无效的。

所有在同一组的端口必须是相同类别的。

Cisco Catalyst 2950-24 交换机只有一个模块，模块编号为 0，该模块有 24 个快速以太网端口。

2．配置端口速率和单双工模式

在默认情况下，交换机的端口速度设置为 auto（自动协商），此时链路的两个端点将交流有关各自能力的信息，从而选择一个双方都支持的最大速度和单工或双工通信模式。可以配置快速以太口的速率为 10/100Mbps 及千兆位以太口的速率为 10/100/1000Mbps，但对于 GBIC 端口则不能配置，其速率及双工模式一般设置为自动协商（auto）。

配置命令为：

```
speed {10 | 100 | 1000 | auto }      //设置端口速率
duplex {auto | full | half}          //设置全双工或半双工
```

auto 代表自动协商模式，full 代表全双工（full-duplex），half 代表半双工（half-duplex）。

3．配置端口描述

在网络实际使用中，可对端口指定描述文字，对端口的功能和用途等进行说明，以起到备忘作用，其配置命令为：

```
description string
```

要删除描述文字，可以使用 no description 命令。

4．监控及维护端口

在交换机的使用过程中，可以监控端口和控制器的状态，主要命令如下：

```
show interfaces [interface-id] status [err-disabled]        //显示端口状态
show interfaces [interface-id] switchport                   //显示二层端口的状态
show interfaces [interface-id] description                  //显示端口描述
show running-config interface [interface-id]                //显示当前配置中的端口配置情况
```

5．启用和禁用端口

对于没有连接的端口，其状态始终处于 shutdown。对于正在工作的端口，可根据管理需要，进行启用或禁用。比如，若发现连接在某端口的计算机正在发送大量攻击类型的数据，此时就可禁用该端口，使该主机从网络上断开。使用 no shutdown 命令可重新打开端口。

例：设置交换机 fastethernet0/3 端口参数。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/3
Switch(config-if)# speed 100                                //端口速率设为 100Mbps
Switch(config-if)# duplex full                              //通信方式为全双工
Switch(config-if)#description Connects to Marketing         //给端口加上描述文字
Switch(config-if)## no shutdown                             //启用端口
Switch(config-if)#end                                       //结束端口配置
Switch#show interfaces fastethernet 0/3                     //查看端口配置
```

6.4.4 交换机VLAN的配置

在 4.3.7 节中已经对虚拟局域网（VLAN）技术做了介绍，本节将介绍基于端口的 VLAN（静态 VLAN）的配置方法。静态 VLAN 是在交换机上手动将交换机的端口分配给不同的 VLAN。当在 Cisco 29xx 系列交换机上配置静态 VLAN 时，必须记住以下准则：

（1）VLAN 的最大数目取决于交换机及交换机的端口的数目。

（2）VLAN1 是出厂时定义的默认 VLAN 之一，VLAN1 是默认的以太网 VLAN。

（3）Cisco 发现协议（CDP）和 VLAN 中继协议（VTP）通告是在 VLAN1 上发送的。

（4）必须给所有参与到 VLAN 中继的交换机配置相同的封装协议（802.1Q 或者 ISL）。

（5）配置 VLAN 的命令随着交换机型号的不同而不同。

（6）Catalyst 29xx 系列交换机的 IP 地址是在 VLAN1 的广播域里。

（7）为了创建、添加或者删除 VLAN，交换机必须配置为 VTP 服务器模式。

1．配置正常范围的VLAN

VLAN 号 1、1002～1005 是自动生成的，不能被去掉。VLAN 号 1～1005 的配置被写到文件 vlan.dat 中，可以用 show vlan 命令查看，vlan.dat 文件存放在 NVRAM 中。

2．创建、修改以太网VLAN

可以通过两种方式来生成、修改以太网 VLAN。

（1）在全局配置模式下进行 VLAN 配置，配置命令为：

```
vlan vlan-id
name vlan-name                    （可选）
```

在 vlan 命令后输入一个 VLAN 号来创建 VLAN。也可给 VLAN 命名，如果没有配置 VLAN 名，默认的名字是 VLAN 号前面用 0 填满的 4 位数，如 VLAN0008 是 VLAN8 的默认名字。

（2）在 VLAN 数据库模式下进行 VLAN 配置，命令如下：

```
vlan database
vlan vlan-id name vlan-name
```

可以使用 show vlan 命令来进行验证，用 no vlan vlan-id 命令来删除 VLAN。

3．为VLAN分配端口

为 VLAN 分配端口是在相应的端口下通过以下命令来实现：

```
switchport access vlan vlan-id
```

可在全局配置模式下使用 default interface interface-id 命令还原端口到默认配置状态。

4．删除VLAN

当删除一个处于 VTP 服务器的交换机上的 VLAN 时，则此 VLAN 将在所有相同 VTP 的交换机上被删除。在透明模式下删除时，只在当前交换机上删除。

注意：当删除一个 VLAN 时，原来属于此 VLAN 的端口将处于非激活的状态，直到将其分配给某一 VLAN。

在全局配置模式下删除 VLAN 的命令为：

```
no vlan vlan-id
```

也可先进入 vlan database，再用 no vlan vlan-id 来删除 VLAN。

例：配置静态 VLAN。

```
Switch# configure terminal                                  //进入全局配置模式
Switch(config)# vlan 10                                     //在全局配置模式下配置 VLAN 号
Switch(config-vlan)# name test10                            //配置 VLAN 名
Switch(config-vlan)# end                                    //退出 VLAN 配置，回到特权模式
Switch#vlan database                                        //进入 VLAN 数据库模式
Switch(vlan)#vlan 20 name test20                            //配置 VLAN 号和 VLAN 名
Switch(vlan)#exit                                           //退出 VLAN 数据库模式，回到特权模式
Switch# configure terminal                                  //进入全局配置模式
Switch(config)# interface range fastethernet0/5-10          //选择要配置的一组端口
Switch(config-if-range)# switchport mode access             //设置为访问连接端口
Switch(config-if range)# switchport access vlan 10          //设置端口属于 vlan 10
Switch(config-if range)#interface range fastethernet0/11-15 //配置 f0/11 ~ f0/15 端口
Switch(config-if range)# switchport mode access             //设置为访问连接端口
Switch(config-if range)# switchport access vlan 20          //设置端口属于 vlan 20
Switch(config-if range)# interface fastethernet0/24         //配置 f0/24 端口
Switch(config-if)# switchport mode access                   //设置为访问连接端口
```

```
Switch(config-if)# switchport access vlan 20        //设置端口属于 vlan 20
Switch(config-if)# end                              //退出端口配置，回到特权模式
Switch#show vlan                                    //查看 VLAN 信息
Switch# copy running-config startup-config          //保存当前配置
```

6.5 路由器的一般配置

6.5.1 路由表与路由协议

1．路由表

路由器的主要功能是，为经过路由器的每一个数据包寻找一条最佳通信路径并将该数据有效地传送到目标节点。选择最佳通信路径是由路由策略（即路由算法）来实现的，路由策略实际上就是路由器中保存的供路由选择时使用的各种传输路径的相关数据（路由表）。

路由表包含子网的标志信息、网络中路由器的数量及下一个路由器的名字等内容，路由器根据路由表中的信息来判断网络地址和选择通信路径，路由器能够在各种不同的网络间建立灵活的连接，以实现不同数据分组和不同介质访问方法的网络或子网间的相互通信。路由表可以由系统管理员手动设置（静态路由表），也可以由系统自动生成或调整（动态路由表）。

1）静态路由表

静态路由表是由系统管理员采用手动方式进行设置的路由表，一般在系统安装时根据网络的拓扑情况而设定，并且不随网络结构的改变而改变。

2）动态路由表

动态路由表是路由器根据网络系统的运行情况自动调整而得到的路由表。路由器根据路由选择协议提供的功能，自动学习并记忆网络实际可用的通信路径，在需要时自动计算并选择数据传输的最佳路径。

2．路由协议

典型的路由选择方式有两种：静态路由和动态路由。

1）静态路由

静态路由是在路由器中设置的固定的路由表。除非网络管理员干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变做出反应，一般用于网络规模不大、拓扑结构固定的网络中。

静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。当动态路由与静态路由发生冲突时，以静态路由为准。

2）动态路由

动态路由是网络中的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由表的过程。它能实时地适应网络结构的变化。如果路由更新信息表明发生了网络变化，路由选择软件就会重新计算路由，并发出新的路由更新信息。动态路由适用于网络规模大、网络拓扑复杂的网络。

根据是否在一个自治系统内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。这里的自治系统指一个具有统一管理机构、统一路由策略的网络。自治系统内部采用的路由选择协议称为内部网关协议，常用的有 RIP、OSPF；外部网关协议主要用于多

个自治系统之间的路由选择，常用的是 BGP 和 BGP-4。

静态路由和动态路由有各自的特点和适用范围，因此，在网络中动态路由通常作为静态路由的补充。当一个分组在路由器中进行寻径时，路由器首先查找静态路由。如果查到，则根据相应的静态路由转发分组；否则，再查找动态路由。

3．RIP

RIP（Routing Information Protocol，路由信息协议）是 Internet 中常用的路由协议。RIP 采用距离向量算法，即路由器根据距离选择路由，所以也称为距离向量协议。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数的路径信息，除到达目的地的最佳路径外，任何其他信息均予以丢弃。同时，路由器也把所收集的路由信息用 RIP 协议通知相邻的其他路由器。这样，正确的路由信息逐渐扩散到全网。

RIP 使用非常广泛，它简单、可靠，便于配置。但是，RIP 只适用于小型的同构网络，因为它允许的最大站点数为 15，任何超过 15 个站点的目的地均被标记为不可达。而且，RIP 每隔 30s 一次的路由信息广播也是造成网络的广播风暴的重要原因之一。

4．OSPF

OSPF 是一种基于链路状态的路由协议，需要每个路由器向其同一管理域的所有其他路由器发送链路状态广播信息。在 OSPF 的链路状态广播中包括所有接口信息、所有的量度和其他一些变量。利用 OSPF 的路由器，首先必须收集有关的链路状态信息，并根据一定的算法计算出到每个节点的最短路径。而基于距离向量的路由协议仅向其邻接路由器发送有关路由更新信息。

与 RIP 不同，OSPF 将一个自治系统再划分为区，即有两种类型的路由选择方式：当源和目的地在同一区时，采用区内路由选择；当源和目的地在不同区时，则采用区间路由选择。这就大大减少了网络开销，并增加了网络的稳定性。当一个区内的路由器出故障时，并不影响自治系统内其他区的路由器正常工作，这也给网络的管理、维护带来方便。

5．BGP和BGP4

BGP 是为 TCP/IP 互联网设计的外部网关协议，用于多个自治系统之间。它既不是基于纯粹的链路状态算法，也不是基于纯粹的距离向量算法。它的主要功能是与其他自治系统的 BGP 交换网络可达信息。各个自治系统可以运行不同的内部网关协议。BGP 更新信息包括网络号和自治系统路径的成对信息。自治系统路径包括到达某个特定网络必须经过的自治系统串，这些更新信息通过 TCP 传送出去，以保证传输的可靠性。

为了满足 Internet 日益扩大的需要，BGP 还在不断地发展。在最新的 BGP4 中，还可以将相似路由合并为一条路由。

6.5.2 路由器的基本配置

路由器的基本配置包括主机名的配置、系统时间和日期的配置、各种接口的配置和启用、路由器口令的配置。

1．主机名的配置

配置路由器主机名与配置交换机的主机名的命令相同，都是在全局配置模式下，使用 hostname 命令实现。

2．系统时间和日期的配置

配置路由器的系统时间和日期的命令是 clock set。系统时间的格式为“时：分：秒”，日

期的格式为“日　月　年”，其中月份必须使用相应月份的英文单词或单词缩写。

例如，配置路由器系统时间和日期为 2008 年 5 月 20 日 19 点 38 分零 32 秒，命令如下：

```
Router#clock set 19:38:32 20 may 2008
```

3．各种接口的配置和启用

路由器上的三种基本接口为局域网（LAN）接口、广域网（WAN）接口和 loopback（回送）接口。在配置接口之前，首先选择相应接口，并进入接口配置模式，然后根据需要进行相关的配置。无论哪种类型的接口，都需要为该接口配置一个 IP 地址，并且要启用该接口，该接口的配置才能生效。

想知道一台路由器有哪些可用的接口，可以用 show interface 命令列出全部的接口信息，或者用 show ip interface brief 命令以简洁的形式列出路由器所有接口的信息。

1）LAN 接口的配置

LAN 接口是路由器与局域网的连接点，每个 LAN 接口与一个子网相连，配置 LAN 接口就是将 LAN 接口子网地址范围内的一个 IP 地址分配给 LAN 接口。配置步骤如下：

（1）进入全局配置模式。

（2）进入接口配置模式。

（3）给指定接口配置 IP 地址和子网掩码。

（4）开启该接口。

例：配置 LAN 接口 f0/0 的 IP 地址并启用该接口。

```
Cisco2611#config t                                          //进入全局配置模式
Cisco2611(config)#interface fastethernet 0/0                //进入接口 f0/0 配置模式
Cisco2611(config-if)#ip address 200.38.118.9 255.255.255.0  //配置接口 IP 地址和子网掩码
Cisco2611(config-if)#no shutdown                            //启动接口
Cisco2611(config-if)#^Z                                     //退出接口配置模式，回到特权 EXEC 模式
Cisco2611#show ip interface f0/0                            //查看接口 f0/0
```

2）WAN 接口的配置

下面以串行接口为例来介绍 WAN 接口的配置方法。串行接口需要时钟信号来控制通信同步。在多数环境中，数据通信设备（DCE）提供该时钟。在默认情况下，Cisco 路由器是数据终端设备（DTE），但可以被配置为 DCE 设备。

在直接相互连接的串行链路上，必须有一侧作为 DCE 并提供时钟信号。通过 clockrate 命令激活时钟并设定其速率。可用的以 bit/s 为单位的时钟速率为 1200、2400、9600、19200、38400、56000、64000、72000、125000、148000、500000、800000、1000000、1300000、2000000 和 4000000。根据功能不同，某些速率在某些串口上是不可用的。

要配置一个串口，需要按如下步骤操作：

（1）在特权模式下，输入 config terminal 命令进入配置模式。

（2）进入所要配置的接口，如串口 0，命令格式为 nterface serial 0，进入接口模式。

（3）配置 IP 地址和子网掩码，输入 ip address 加 IP 地址和子网掩码。

（4）设置 DCE 时钟速率（在 DTE 上跳过此步）。

（5）用 no shutdown 开启该接口。

（6）按 Ctrl+Z 键结束接口配置，返回特权模式。

（7）可用 show interface s0 命令来查看串口配置。

例：串行接口 s0/0 为 DCE，配置 s0/0。

```
Cisco2611#config t                                          //进入配置模式
Cisco2611(config)#interface s0/0                            //进入所要配置的接口 s0/0
Cisco2611(config-if)#ip address 210.10.23.1 255.255.255.254 //配置 IP 地址和子网掩码
Cisco2611(config-if)#bandwidth 56                           //配置接口带宽
Cisco2611(config-if)#clockrate 56000                        //设置 DCE 时钟速率
Cisco2611(config-if)#no shutdown                            //启用接口
```

在默认情况下，路由器的接口是关闭的，必须用 no shutdown 命令来开启路由器的接口。

4．路由器口令的配置

路由器口令的配置包括特权密码、Console 端口和 VTY 端口密码。

配置特权密码是在全局配置模式下，使用如下命令：

```
enable password password          //配置采用明文方式保存的密码
enable secret password            //配置采用加密方式保存的密码
```

配置本地 Console 和 VTY 端口密码是在线路模式下使用如下命令：

```
password password
login
```

为了防止空闲的连接长时间地存在，通常还应配置 Console 和 VTY 线路的空闲超时时间，默认空闲超时时间为 10min。配置空闲超时时间的命令为：

```
exec-timeout minute second
```

例：设置路由器采用加密保存的特权密码为 router_enable，Console 端口登录密码为 router_console，VTY 线路 0～4 登录密码为 router_vty，Console 和 VTY 线路空闲超时时间为 3min。

```
Router#config t                                  //进入配置模式
Router(config)#enable secret router_enable       //设置加密保存的特权密码
Router(config)#line console 0                    //进入 console 线路配置模式
Router(config-line)#password router_console      //设置 console 密码
Router(config-line)#login                        //启用密码验证
Router(config-line)#exec-timeout 3 0             //配置线路空闲超时时间
Router(config-line)#exit                         //退出 console 配置模式
Router(config)#line vty 0 4                      //进入 VTY 线路配置模式
Router(config-line)#password router_console      //设置 VTY 线路远程登录密码
Router(config-line)#login                        //启用密码验证
Router(config-line)#exec-timeout 3 0             //配置线路空闲超时时间
Router(config-line)#end                          //退出配置模式
Router#show run                                  //查看当前配置
```

6.5.3　路由协议配置

1．静态路由配置

1）静态路由配置的步骤及命令

静态路由的操作可以总结为三个步骤：

（1）网络管理员根据网络拓扑配置路由。

（2）路由器将路由装入路由器选择表。

（3）使用静态路由进行路由分组。

因为静态路由是由管理员手工配置的，所以必须在路由器上使用 ip route 命令配置静态路由。建立静态路由的命令为：

```
Router(config)#ip route prefix mask {address | interface} [distance]
```

参数说明

Prefix：所要到达的目的网络。

mask：子网掩码。

address：下一个跳的 IP 地址，即相邻路由器的端口地址。

interface：本地出站网络接口。

distance：管理距离（可选），管理距离越小表示路由越可靠。

在一条静态路由中，address 和 interface 只能选择其中之一，使用本地出站网络接口（interface）比使用下一个跳的 IP 地址（address）效率更高，因为路由选择表中的路由最终会解析为出站接口。

例：下面以图 6.14 所示的简单网络为例来介绍静态路由的配置。

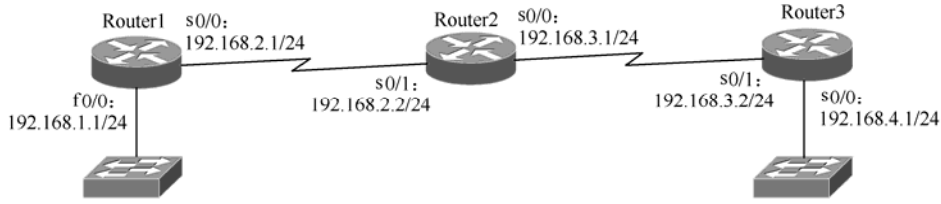


图 6.14　静态路由配置拓扑

3 台路由器的静态路由配置如下。

Router1：

```
Router1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
Router1(config)#ip route 192.168.4.0 255.255.255.0 192.168.2.2
```

Router2：

```
Router2(config)#ip route 192.168.1.0 255.255.255.0 s0/1
Router2(config)#ip route 192.168.4.0 255.255.255.0 s0/0
```

Router3：

```
Router3(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
Router3(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.1
```

其中，Router1 和 Router3 使用下一跳地址，Router2 使用出站网络接口。

2）默认路由的配置

默认路由用来路由那些目的网络不匹配路由表中的任何一条其他路由的分组，它是一条特殊的静态路由。只要没有在路由表里找到去特定目的地址的路径，数据就被路由到默认路由指定的相邻路由器。默认路由的格式如下：

```
ip route 0.0.0.0 0.0.0.0 [next-hop-address | outgoing interface]
```

目的网络地址为 0.0.0.0，子网掩码为 0.0.0.0，默认路由的 address 参数可以是连接外部网

络的本地路由器接口，也可以是下一跳路由器的 IP 地址。

在图 6.14 中，由于 Router1 除了与 Router2 相连外，不再与其他路由器相连，所以可以为它赋予一条默认路由以代替以上两条静态路由。默认路由的格式如下：

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

Router3 也同样可以使用如下默认路由的格式来代替原来的两条静态路由：

```
Router3(config)#ip route 0.0.0.0 0.0.0.0 s0/1
```

3）静态路由的检验

配置完静态路由后，检验静态路由的配置以及路由表中的静态路由是否像期望的那样工作是很重要的。使用 show running-config 命令来查看当前运行的配置以检验静态路由的输入是否正确。使用 show ip route 命令以确保静态路由在路由表中存在。使用 ping 命令来测试能否到达目的网络。

可使用以下步骤对静态路由配置进行故障排除：

（1）确定该路由作为网关的链路是可用的。

（2）输入 show interfaces，检验这个接口的状态是 up，链路协议状态是 up。

（3）检验接口所使用的 IP 地址是否正确。

（4）ping 直连的远程路由器的接口 IP 地址。如果 ping 不通，则可能是直连的路由器的一个或两个接口配置不正确，或者链路存在物理故障。返回第（1）步进行故障排除。

（5）如果 ping 远端路由器失败，使用 traceroute 命令来确认路由路径上的哪个路由器在丢弃分组。

（6）登录到 traceroute 失败的路由器上，返回第（1）步重新开始排除故障。

（7）如果 ping 成功了，尝试 ping 远端路由器。如果这次 ping 成功，则说明端到端的连通性已经达到。静态路由的测试完成。

2．RIP配置

1）RIP 的配置命令

在全局配置模式下使用表 6.3 中的命令来配置 RIP。

表 6.3　启用 RIP 的命令

任　务	命　令
启动一个 RIP 路由选择进程	Route(config)#router rip
指定 RIP 版本	Route(config)#version {1|2}
指定与 RIP 路由选择关联的网络	Route(config)#network network-number

注：RIP 版本 2 支持验证、密钥管理、路由汇总、无类域间路由（CIDR）和变长子网掩码（VLSM）。

2）RIP 配置举例

例：配置如图 6.15 所示的网络的 RIP 协议

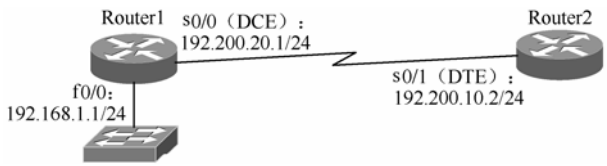


图 6.15　RIP 配置举例的网络拓扑

Router1：

```
Router1(config)#router rip                          //启用 RIP 路由协议
Router1(config-router)#version 2                    //指定 RIP 版本
Router1(config-router)#network 192.200.10.0         //指定与 RIP 路由选择关联的网络
Router1(config-router)#network 192.168.1.0          //指定与 RIP 路由选择关联的网络
```

Router2：

```
Router2(config)#router rip                          //启用 RIP 路由协议
Router2(config-router)#version 2                    //指定 RIP 版本
Router2(config-router)#network 192.200.10.0         //指定与 RIP 路由选择关联的网络
```

RIP 的 network 命令只使用有类地址或主网络地址。如果一个或多个接口已经子网化，则只使用具有有类网络地址的单个 network 命令。如果使用子网地址，IOS 会将其转换成有类地址，用命令 show running-config 可看到。

3）RIP 配置的检验

配置好 RIP 后，可以使用 show ip protocol 和 show ip route 命令来检验是否正确配置了 RIP，用 debug ip rip 命令观察 RIP 路由选择活动。

（1）show ip protocol。在特权模式下，使用 show ip protocol 命令输出配置在路由器上的所有 IP 路由选择协议信息。通过该命令可以检验是否配置了 RIP、是否从正确的接口发送和接收 RIP 更新、发送和接收的是正确的 RIP 版本、路由器通告了正确的网络等。

（2）show ip route。在特权模式下，使用 show ip route 命令可以检验路由表中的 RIP 路由。在该命令的输出查看标记为“R”的路由就是 RIP 路由。注意，由于网络要经过一段时间才能收敛，因此这些路由不会立即出现在路由表中。

（3）debug ip rip。用来发现 RIP 更新问题的主要方法是在特权模式下使用 debug ip rip 命令，它显示发送和接收到的 RIP 路由选择更新。用 no debug ip rip 来终止调试命令。

3．配置OSPF

1）OSPF 相关概念和术语

（1）链路状态（Link-State）：OSPF 路由器收集所在网络区域上各路由器的连接状态信息，即链路状态信息，生成链路状态数据库。路由器掌握了该区域上所有路由器的链路状态信息，也就了解了整个网络的拓扑结构。OSPF 路由器利用最短路径优先算法（Shortest Path First，SPF）独立计算到达任意目的网络的路由。

（2）区域（Area）：OSPF 网络分为多个部分，称为“区域（Area）”，可以高效地控制网络运行。每个区域就如同一个独立的网络，该区域的 OSPF 路由器只保存本区域的链路状态。区域 0 是主区域。所有 OSPF 网络都有一个区域 0，而且它也作为主分配区。

（3）指定路由器（Designated Router，DR）和备份指定路由器（Backup Designated Router，BDR）：在多路访问网络上可能存在多个路由器，为了减少在同一个区域中相邻路由器互相交换信息的数量，OSPF 要求在区域中选举一个 DR。每个路由器都与 DR 建立完全相邻关系。DR 负责收集所有的链路状态信息，并发布给其他路由器。在选举 DR 的同时，也选举出一个 BDR，当 DR 失效时，BDR 担负起 DR 的职责。

2）配置 OSPF 的有关命令

配置 OSPF 路由协议是在全局配置模式下，使用表 6.4 中的命令来实现。

表 6.4　配置 OSPF 的有关命令

任　务	命　令
启用 OSPF 协议	router ospf process-id①
标志参与 OSPF 的网络	network address wildcard-mask area area-id②
指定与该路由器相邻的节点地址	neighbor ip-address

注：① OSPF 路由进程 process-id 必须指定范围为 1～65535，多个 OSPF 进程可以在同一个路由器上配置，但最好不这样做。多个 OSPF 进程需要多个 OSPF 数据库的副本，必须运行多个最短路径算法的副本。process-id 只在路由器内部起作用，不同路由器的 process-id 可以不同。

② wildcard-mask 是子网掩码的反码，网络区域 ID area-id 为 0～4294967295 内的十进制数，也可以是带有 IP 地址格式的 x.x.x.x。当网络区域 ID 是 0 或 0.0.0.0 时为主干域。不同网络区域的路由器通过主干域学习路由信息。

3）配置环回地址

当 OSPF 进程启动时，如果配置了环回（loopback）接口的 IP 地址，路由器将使用环回接口地址作为 OSPF 路由器的 ID；否则使用最高的本地 IP 地址作为其 OSPF 路由器的 ID。

配置环路接口的命令如下：

```
Router(config)#interface loopback number
Router(config-if)#ip address ip-addrsss subnet-mask
```

使用环回地址作为路由器的 ID 可以确保稳定性，因为环回接口不会出现链路失效的情况。要使用环回地址作为路由器的 ID，该环回接口必须在 OSPF 进程开始之前配置。

建议在所有基于 OSPF 的网络中的关键路由器都使用环回地址。为了避免路由选择问题，在配置环回地址时最好配置一个 32 位的子网掩码。例如：

```
Router(config)#interface loopback 0
Router(config-if)#ip address 211.156.10.1 255.255.255.255
```

32 位的掩码通常称为主机掩码，因为它是指定一个主机，而不是一个网络或子网。

4）基本 OSPF 配置举例

例：配置如图 6.16 所示的网络的 OSPF。

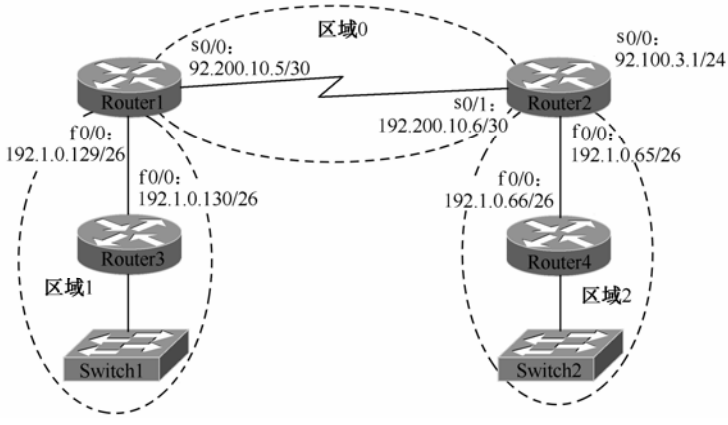


图 6.16　基本 OSPF 配置的网络拓扑

Router1：

```
Router1(config)#interface fastethernet 0/0                    //进入接口 f0/0 配置
Router1(config-if)#ip address 192.1.0.129 255.255.255.192     //配置 f0/0 的 IP 地址
Router1(config-if)#no shutdown                                //启用接口
Router1(config-if)#interface serial 0/0                       //进入接口 s0/0 配置
Router1(config-if)#ip address 192.200.10.5 255.255.255.252    //配置 s0/0 的 IP 地址
Router1(config-if)#no shutdown                                //启用接口
Router1(config-if)#exit                                       //退出接口配置模式
Router1(config)#router ospf 100                               //启用 OSPF 协议
Router1(config-router)#network 192.200.10.4 0.0.0.3 area 0    //标志参与 OSPF 的网络
Router1(config-router)#network 192.1.0.128 0.0.0.63 area 1    //标志参与 OSPF 的网络
```

Router2：

```
Router2(config)#interface fastethernet 0/0                    //进入接口 f0/0 配置
Router2(config-if)#ip address 192.1.0.65 255.255.255.192      //配置 f0/0 的 IP 地址
Router2(config-if)#no shutdown                                //启用接口
Router2(config-if)#interface serial 0/1                       //进入接口 s0/1 配置
Router2(config-if)#ip address 192.200.10.6 255.255.255.252    //配置 s0/1 的 IP 地址
Router2(config-if)#no shutdown                                //启用接口
Router2(config-if)#exit                                       //退出接口配置模式
Router2(config)#router ospf 200                               //启用 OSPF 协议
Router2(config-router)#network 192.200.10.4 0.0.0.3 area 0    //标志参与 OSPF 的网络
Router2(config-router)#network 192.1.0.64 0.0.0.63 area 2     //标志参与 OSPF 的网络
```

Router3：

```
Router3(config)#interface fastethernet 0/0                    //进入接口 f0/0 配置
Router3(config-if)#ip address 192.1.0.130 255.255.255.192     //配置 f0/0 的 IP 地址
Router3(config-if)#no shutdown                                //启用接口
Router3(config-if)#exit                                       //退出接口配置模式
Router3(config)#router ospf 300                               //启用 OSPF 协议
Router3(config-router)#network 192.1.0.128 0.0.0.63 area 1    //标志参与 OSPF 的网络
```

Router4：

```
Router4(config)#interface fastethernet 0/0                    //进入接口 f0/0 配置
Router4(config-if)#ip address 192.1.0.66 255.255.255.192      //配置 f0/0 的 IP 地址
Router4(config-if)#no shutdown                                //启用接口
Router4(config-if)#exit                                       //退出接口配置模式
Router4(config-router)#router ospf 400                        //启用 OSPF 协议
Router4(config-router)#network 192.1.0.64 0.0.0.63 area 2     //标志参与 OSPF 的网络
```

5）OSPF 的监控和调试命令

show ip route：显示路由表。

show ip ospf：显示 SPF 执行的次数以及链路状态的更新时间间隔。

show ip ospf database：显示路由器维护的拓扑数据库的内容。

show ip ospf interface：检验已经配置在目标的区域中的接口。

show ip ospf neighbor detail：显示邻居路由器的详细信息。

clear ip route：清除路由表中的路由。

debug ip ospf：调试监控 OSPF 协议的运行。

6.5.4 广域网协议配置

本节介绍在 Cisco 路由器上的 PPP、X.25、帧中继协议配置。

1．PPP

1）PPP 简介

PPP（Point-to-Point Protocol，点到点协议）是 SLIP（Serial Line IP protocol，串行线路 IP 协议）的继承者，它提供了跨过同步和异步电路实现路由器到路由器（Router-to-Router）和主机到网络（Host-to-Network）的连接。该协议提供在链路层的全双工操作，并按照顺序传递数据包。由于 PPP 具有简单、动态 IP 地址分配、可对传输数据进行压缩和入网用户认证等优点，因而成为广域网上使用非常广泛的协议之一。它主要用于家庭拨号上网、ADSL 上网、局域网和点对点连接等。

CHAP（Challenge Handshake Authentication Protocol，竞争握手认证协议）和 PAP（Password Authentication Protocol，口令认证协议）通常用于在 PPP 封装的串行线路上提供安全性认证。使用 CHAP 和 PAP 认证，每个路由器通过名字来识别，可以防止未经授权的访问。

2）配置 PPP 的步骤

（1）配置本地路由器名称。

（2）配置本地路由器口令。

（3）配置对端路由器的名称和口令。

（4）封装 PPP。

（5）指定 PPP 的认证方式。

3）配置 PPP 的有关命令

在端口配置模式下，使用表 6.5 中的有关命令。

表 6.5　配置 PPP 的有关命令

任　务	命　令
封装 PPP	encapsulation ppp
配置认证方式	ppp authentication {chap | chap pap | pap chap | pap} [list-name | default] [callin]
指定用户名和口令	username name password secret
配置 DCE 端线路速度	clockrate speed

注意：要使用 CHAP/PAP，必须使用 PPP 封装。在与非 Cisco 路由器连接时，一般采用 PPP 封装，其他厂家的路由器一般不支持 Cisco 的 HDLC 封装协议。

4）PPP 配置实例

例：在如图 6.17 所示的网络中， Router1 和 Router2 的 s0/0 口均封装 PPP，采用 CHAP 做认证，在 Router1 中应建立一个用户，以对端路由器主机名作为用户名，即用户名应为 Router2。同时在 Router2 中应建立一个用户，以对端路由器主机名作为用户名，即用户名应为 Router1。所建的这两个用户的 password 必须相同。

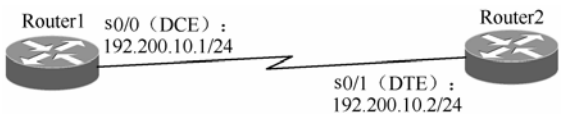


图 6.17　PPP 配置实例

（1）Router1 配置：

```
Router1#configure terminal                                  //进入全局配置模式
Router1(config)#hostname Router1                            //配置 Router1 的主机名
Router1(config)#enable secret Router1                       //配置 Router1 的密码
Router1(config)#username router2 password cec-ppp           //设置对端拨号用户名和密码
Router1(config)#interface serial0/0                         //进入接口 s0/0 配置
Router1(config-if)#ip address 192.200.10.1 255.255.255.0    //配置接口 s0/0 的 IP 地址
Router1(config-if)#encapsulation ppp                        //封装 PPP
Router1(config-if)#clockrate 2000000                        //配置 DCE 时钟
Router1(config-if)#ppp authentication chap                  //配置认证协议
Router1(config-if)#no shutdown                              //启用接口
```

（2）Router2 配置：

```
Router2(config)#hostname Router2                            //配置 Router2 的主机名
Router1(config)#enable secret Router2                       //配置 Router2 的密码
Router2(config)#username router1 password cec-ppp           //设置对端拨号用户名和密码
Router2(config)#interface Serial0/1                         //进入接口 s0/1 配置
Router2(config-if)#ip address 192.200.10.2 255.255.255.0    //配置接口 s0/1 的 IP 地址
Router2(config-if)#encapsulation ppp                        //封装 PPP
Router2(config-if)#ppp authentication chap                  //配置认证协议
Router2(config-if)#no shutdown                              //启用接口
```

配置完成后，可用 debug ppp authentication 来检测配置结果。

2．X.25 配置

1）X.25 配置的步骤

（1）配置端口 IP 地址。

（2）设置 X.25 封装。

（3）设置本地路由器端口 X.121 地址。

（4）设置 X.25 最大的双向虚电路数，如果省略此步，表示使用默认值 1。

（5）设置一次连接可同时建立的虚电路数。

（6）设置对端路由器的 IP 与 X.121 映射地址。

（7）设置 X.25 在清除空闲虚电路前的等待时间，如果省略此步，表示使用默认值 0，即一旦建立虚电路，将不清除该连接。

（8）重新启动 X.25，或清除一个 svc，启动一个 pvc 相关参数。

（9）显示接口及 X.25 相关信息。

2）X.25 配置的相关命令

X.25 配置的相关命令如表 6.6 所示。

表 6.6　X.25 配置的相关命令

任　务	命　令
设置 X.25 封装	encapsulation x25 [dce]
设置 X.121 地址	x25 address x.121-address

续表

任　务	命　令
设置对端路由器的映射地址	x25 map protocol address [protocol2 *address2*[...[protocol9 address9]]] x121-address [option]
设置最大的双向虚电路数	x25 htc circuit-number①
设置一次连接可同时建立的虚电路数	x25 nvc count②
设置 X.25 在清除空闲虚电路前的等待时间	x25 idle minutes
重新启动 X.25，或清除一个 svc，启动一个 pvc 相关参数	clear x25 {serial number | cmns-interface mac-address} [vc-number]③
清除 X.25 虚电路，启动 pvc	clear x25-vc
显示接口及 X.25 相关信息	show interfaces serial show x25 interface show x25 map show x25 vc

注：① 虚电路号从 1 到 4095，Cisco 路由器默认为 1024，国内一般分配为 16。

② 电路计数从 1 到 8，默认为 1。

③ 在改变了 X.25 各层的相关参数后，应重新启动 X.25（使用 clear X.25 {serial number | cmns-interface mac-address} [vc-number]或 clear x25-vc 命令），否则新设置的参数可能不生效。同时，应对照服务提供商对于 X.25 交换机端口的设置来配置路由器的相关参数。若出现参数不匹配，则可能导致连接失败或其他意外情况。

3）X.25 配置实例

在如图 6.17 所示的网络中，将路由器 Router1 和路由器 Router2 改用 X.25 协议进行点到点通信。路由器设置如下：

Router1：

```
Router1#configure terminal                              //进入全局配置模式
Router1(config)#interface serial0/0                     //进入接口 s0/0 配置
Router1(config-if)#ip address 192.200.10.1 255.255.255.0  //配置 s0/0 的 IP 地址
Router1(config-if)#clockrate 2000000                    //配置 DCE 时钟
Router1(config-if)#encapsulation x25 dte                //封装 X.25 协议
Router1(config-if)#x25 address 100                      //配置 X.121 地址
Router1(config-if)#x25 htc 16                           //设置最大的双向虚电路数
Router1(config-if)#x25 nvc 2                            //设置一次连接可同时建立的虚电路数
Router1(config-if)#x25 map ip 192.200.10.2 101          //设置对端（Router2）的映射地址
Router1(config-if)#no shutdown                          //启用端口
```

Router2：

```
Router2#configure terminal                              //进入全局配置模式
Router2(config)#interface serial0/1                     //进入接口 s0/1 配置
Router2(config-if)#ip address 192.200.10.2 255.255.255.0  //配置 s0/1 的 IP 地址
Router2(config-if)#encapsulation x25 dte                //封装 X.25 协议
Router2(config-if)#x25 address 101                      //配置 X.121 地址
Router2(config-if)#x25 htc 16                           //设置最大的双向虚电路数
Router2(config-if)#x25 nvc 2                            //设置一次连接可同时建立的虚电路数
```

```
Router2(config-if)#x25 map ip 192.200.10.1 100          //设置对端（Router1）的映射地址
Router2(config-if)#no shutdown                          //启用端口
```

在 Router1 中 ping Router2 的 s0/1 接口 IP 地址，如能 ping 通，则表明配置成功。

3．帧中继网络配置

1）帧中继配置的有关命令

帧中继配置的有关命令如表 6.7 所示。

表 6.7　帧中继配置的有关命令

任　务	命　令
设置 Frame Relay 封装	encapsulation frame-relay [cisco | ietf]①
设置 Frame Relay LMI 类型	frame-relay lmi-type {ansi | cisco | q933a}②
设置子接口	interface interface-type interface-number.subinterface-number [multipoint | point-to-point]
映射协议地址与 DLCI	frame-relay map protocol protocol-address dlci [broadcast]③
设置 FR DLCI 编号	frame-relay interface-dlci dlci [broadcast]
显示 LMI 相关信息	show frame-relay lmi
显示网络协议和 DLCI 的映射	show frame-relay map
显示 PVC 的相关信息	show frame-relay pvc
显示帧中继传输状态	show frame-relay route

注：① 若使 Cisco 路由器与其他厂家的路由设备相连，则使用 Internet 工程任务组（IETF）规定的帧中继封装格式。

② 从 Cisco IOS 版本 11.2 开始，软件支持本地管理接口（LMI）“自动感觉”，“自动感觉”使接口能确定交换机支持的 LMI 类型，用户可以不明确配置 LMI 接口类型。

③ broadcast 选项允许在帧中继网络上传输路由广播信息。

2）配置实例

Router1 和 Router2 连接成帧中继点对点，相关参数如图 6.18 所示。

图 6.18　帧中继点对点配置实例

路由器设置如下。

Router1：

```
Router1(config)#interface serial 0/0                          //进入 s0/0 接口配置
Router1(config-if)#encapsulation frame-relay                  //设置 Frame Relay 封装
Router1(config-if)#interface serial 0/0.1 point-to-point      //进入子接口点到点配置
Router1(config-subif)#ip address 192.200.10.1 255.255.255.0   //配置子接口 IP 地址
Router1(config-subif)#frame-relay interface-dlci 102          //配置子接口的 DLCI 号
Router1(config-subif)#frame-relay map ip 192.200.10.2 201 broadcast
//映射协议地址和 DLCI 号
Router1(config-subif)#no shutdown                             //启用接口
```

Router2：

```
Router2(config)#interface serial 0/0                                    //进入 s0/0 接口配置
Router2(config-if)#encapsulation frame-relay                            //设置 Frame Relay 封装
Router2(config-if)#interface serial 0/0.1 point-to-point                //进入子接口配置模式
Router2(config-subif)#ip address 192.200.10.1 255.255.255.0             //配置子接口 IP 地址
Router2(config-subif)#frame-relay interface-dlci 201                    //配置子接口的 DLCI 号
Router2(config-subif)#frame-relay map ip 192.200.10.1 102 broadcast
//映射协议地址和 DLCI 号
Router2(config-subif)#no shutdown                                       //启用接口
```

6.5.5 NAT配置与局域网访问Internet

随着 Internet 的网络迅速发展，很多组织使用 IP 网来连接，但又不希望他们所有的主机都暴露给 Internet，同时 IP 地址短缺已成为一个十分突出的问题。为了解决这个问题，出现了多种解决方案。本节介绍一种在目前网络环境中比较有效的方法，即网络地址转换（NAT）功能。

1．NAT概述

NAT（Network Address Translation，网络地址转换）是指在一个网络内部，根据需要可以随意自定义私有 IP 地址，而不需要经过申请。在网络内部，各计算机间通过内部的私有 IP 地址进行通信。当内部的计算机要与外部 Internet 网络进行通信时，具有 NAT 功能的设备（如路由器）负责将其内部的私有 IP 地址转换为合法的公网 IP 地址（即从 ISP 申请的 IP 地址）进行通信。RFC1918 定义的私有 IP 地址如表 6.8 所示。

表 6.8　RFC1918 定义的私有 IP 地址

IP 地址类别	RFC1918 私有地址范围	无类别域(CIDR)前缀
A	10.0.0.0 ~ 10.255.255.255	10.0.0.0/8
B	172.16.0.0 ~ 172.31.255.255	172.16.0.0/12
C	192.168.0.0 ~ 192.168.255.255	192.168.0.0/16

1）NAT 的应用环境

一般来说，在下列两种情况下需要使用 NAT。

（1）一个企业申请的合法 Internet IP 地址很少，而内部网络用户很多。可以通过 NAT 功能实现多个用户同时公用一个合法 IP 与外部 Internet 进行通信。

（2）一个企业不想让外部网络用户知道自己的网络内部结构，可以通过 NAT 将内部网络与外部 Internet 隔开，则外部用户根本不知道通过 NAT 设置的内部 IP 地址。

2）设置 NAT 所需路由器的硬件和软件要求

在硬件方面设置 NAT 功能的路由器至少要有一个内部端口（Inside）和一个外部端口（Outside）。内部端口一般使用路由器的以太网端口，连接内部网络用户，使用的是内部 IP 地址。外部端口可以为路由器上的任意端口，外部端口连接到 ISP，使用的是公网 IP 地址。

在软件方面设置 NAT 功能的路由器的 IOS 应支持 NAT 功能。

3）NAT 的几个术语

在 NAT 中，必须正确理解 4 个地址术语（Inside Local、Inside Global、Outside Local 和

Outside Global）。Inside 是指企业或机构内部所拥有的内部网络，这些网络上的主机通常分配了私有 IP 地址，这些地址不能直接在 Internet 上路由，从而也就不能直接用于对 Internet 的访问，必须通过网络地址转换，以合法 IP 的身份来访问 Internet。内部网络中分配的不能直接访问 Internet 的 IP 地址即 Inside Local 地址。内部网络中分配的能直接访问 Internet 的 IP 就是 Inside Global 地址。Outside（外部）是指除了内部网络之外的所有网络，即 Internet。Global（全局）是指能在 Internet 上通信的地址。理解了 Inside、Outside、Local 和 Global 4 个词的含义后，就不难理解下列几个术语。

（1）内部本地地址（Inside Local Address）：分配给内部网络中的计算机的内部 IP 地址。这些地址通常不是合法的 IP 地址，不能直接在 Internet 上路由。

（2）内部全局地址（Inside Global Address）：对外进行 IP 通信时，代表一个或多个内部本地地址的合法 IP 地址。申请才可取得的 IP 地址。

（3）外部本地地址（Outside Local Address）：外部网络主机使用的 IP 地址。这些地址是公网 IP 地址，但可在内部网络中路由，即对内部网络是可见的。

（4）外部全局地址（Outside Global Address）：外部网络主机使用的 IP 地址。这些地址也是公网 IP 地址，但这些地址对内部网络是不可见的。

2．NAT的分类

NAT 可以分为静态地址转换、动态地址转换、端口地址转换。

1）静态地址转换

静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有 E-mail 服务器或 FTP 服务器等可以为外部用户提供的服务，这些服务器的 IP 地址必须采用静态地址转换，以便外部用户可以使用这些服务。

2）动态地址转换

动态地址转换也是将本地地址与内部合法地址一对一的转换，但是动态地址转换是从内部合法地址池中动态地选择一个未使用的地址对内部本地地址进行转换。

3）端口地址转换（PAT）

端口地址转换 PAT（Port Address Translation）也称为复用动态地址转换。端口地址转换首先是一种动态地址转换，但是它可以允许多个内部本地地址共用一个内部合法地址。地址复用被启用时，路由器在高层协议（如 TCP 或 UDP 端口号）惟一标志某台计算机，将全局地址转化为本地地址。只申请到少量 IP 地址但却经常同时有多于合法地址个数的用户上外部网络的情况，这种转换极为有用。

3．NAT配置步骤及命令

1）静态地址转换基本配置步骤及命令

（1）在内部本地地址与内部合法地址之间建立静态地址转换。在全局设置状态下输入：

```
ip nat inside source static local-ip global-ip
```

（2）指定连接网络的内部端口。在端口设置状态下输入：

```
ip nat inside
```

（3）指定连接外部网络的外部端口。在端口设置状态下输入：

```
ip nat outside
```

注：可以根据实际需要定义多个内部端口及多个外部端口。

2）动态地址转换基本配置步骤及命令

（1）在全局设置模式下，定义内部合法地址池。

```
ip nat pool pool-name start-ip end-ip {netmask netmask | prefix-length prdfix-length}
```

其中，pool-name 是地址池名称，可以任意设定。start-ip 和 end-ip 是地址池的起始地址和结束地址。netmask 用于指定子网掩码，prefix-length 是子网掩码的长度，与使用掩码的效果一样。

（2）在全局设置模式下，定义一个标准的 access-list 规则，以允许哪些内部地址可以进行动态地址转换。

```
access-list access-list-number permit source-ip-address wildcard-mask
```

其中，标号 access-list-number 为 1～99 之间的整数。

（3）在全局设置模式下，将由 access-list 指定的内部本地地址与指定的内部合法地址池进行地址转换。

```
ip nat inside source list access-list-number pool pool-name
```

（4）在端口设置状态下，指定与内部网络相连的内部端口。

```
ip nat inside
```

（5）指定与外部网络相连的外部端口：

```
ip nat outside
```

3）PAT 基本配置步骤及命令

（1）在全局设置模式下，定义内部合法地址池：

```
ip nat pool pool-name start-ip end-ip {netmask netmask | prefix-length prdfix-length}
```

（2）在全局设置模式下，定义一个标准的 access-list 规则，以允许哪些内部本地地址可以进行动态地址转换。

```
access-list access-list-number permit source-ip-address wildcard-mask
```

（3）在全局设置模式下，设置在内部的本地地址与内部合法 IP 地址间建立复用动态地址转换。

```
ip nat inside source list access-list-number pool pool-name overload
或 ip nat inside source list access-list-number interface outside-interface
```

注：如果使用后一条命令就不需要定义地址池，即不需要步骤（1）。

（4）在端口设置状态下，指定与内部网络相连的内部端口：

```
ip nat inside
```

（5）在端口设置状态下，指定与外部网络相连的外部端口：

```
ip nat outside
```

4．NAT的配置举例

1）静态地址转换实例

在如图 6.19 所示的网络中，实现静态 NAT 地址转换功能。将 Router 的快速以太网接口作为内部接口，串行接口 s0/0 作为外部接口。其中，192.168.1.2、192.168.1.3、192.168.1.4 的内部本地地址采用静态地址转换，其内部合法地址分别对应为 220.123.10.2、220.123.10.3、220.123.10.4。

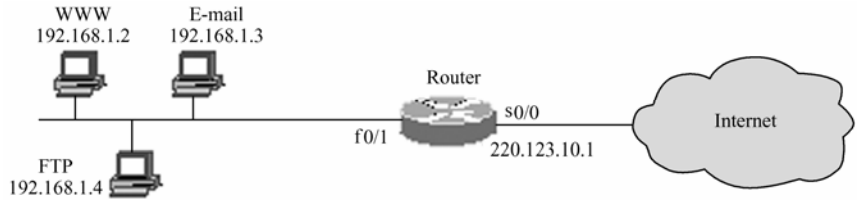


图 6.19　静态 NAT 配置

路由器 Router 的配置如下：

```
Router#config t                                          //进入全局配置模式
Router(config)#ip nat inside source static 192.168.1.2 220.123.10.2
Router(config)#ip nat inside source static 192.168.1.3 220.123.10.3
Router(config)#ip nat inside source static 192.168.1.4 220.123.10.4
//以上 3 条配置静态地址映射关系
Router(config)#interface FastEthernet 0/0                //进入接口 f0/0 配置
Router(config-if)#ip address 192.168.1.1 255.255.255.0   //配置接口 f0/0 的 IP 地址
Router(config-if)#ip nat inside                          //配置接口 f0/0 为内部接口
Router(config-if)#no shutdown                            //启动接口
Router(config-if)#interface Serial 0/0                   //进入接口 s0/0 配置
Router(config-if)#ip address 220.123.10.1 255.255.255.0  //配置接口 s0/0 的 IP 地址
Router(config-if)#ip nat outside                         //配置接口 s0/0 为外部接口
Router(config-if)#no shutdown                            //启动接口
Router(config-if)#exit                                   //退出接口配置模式，回到全配置模式
Router(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0        //默认路由
Router(config)#end                                       //回到特权 EXEC 模式
Router#show ip nat statistics                            //查看 NAT 统计
Router#show ip nat translations                          //查看 NAT 转换详情
```

注：（1）如果内网没有向外网发送数据，用 show ip nat translations 命令看不到转换信息。

（2）可以使用 debug ip nat 命令来监视 NAT 转换的过程，用 no debug ip nat 命令结束监视。

2）动态地址转换实例

在如图 6.20 所示的网络中，运用动态 NAT 地址转换功能。将 Router 的快速以太网接口作为内部接口，串行接口 s0/0 作为外部接口。其中 192.168.1.0/24 网段采用动态地址转换。对应内部合法地址为 220.123.10.2～220.123.10.10。

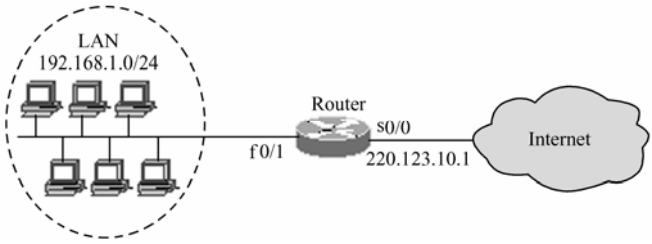


图 6.20　动态地址转换

```
Router#configure terminal                                    //进入全局配置模式
Router(config)#ip nat pool mynat 220.123.10.2 220.123.10.10 netmask 255.255.255.0
//配置内部全局地址池
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
//配置允许地址转换的内部本地地址范围
Router(config)#ip nat inside source list 10 pool mynat
//配置内部本地地址与内部全局地址的映射关系
Router(config)#interface FastEthernet 0/0                    //进入接口 f0/0 配置
Router(config-if)#ip address 192.168.1.1 255.255.255.0       //配置接口 f0/0 的 IP 地址
Router(config-if)#ip nat inside                              //配置接口 f0/0 为内部接口
Router(config-if)#no shutdown                                //启动接口
Router(config-if)#interface Serial 0/0                       //进入接口 s0/0 配置
Router(config-if)#ip address 220.123.10.1 255.255.255.0      //配置接口 s0/0 的 IP 地址
Router(config-if)#ip nat outside                             //配置接口 s0/0 为外部接口
Router(config-if)#no shutdown                                //启动接口
Router(config-if)#exit                                       //退出接口配置模式，回到全配置模式
Router(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0            //默认路由
Router(config)#end                                           //回到特权 EXEC 模式
```

3）端口地址转换（PAT）实例

使用图 6.20 的网络，应用了端口地址转换功能，将 Router 的快速以太网接口作为内部接口，串行接口 s0/0 作为外部接口。192.168.1.0/24 网段采用 PAT。假设企业只申请了一个合法的 IP 地址 220.123.10.1。

路由器 Router 的配置：

```
Router#configure terminal                                    //进入全局配置模式
Router(config)#ip nat pool abc 220.123.10.1 220.123.10.1 netmask 255.255.255.0
//配置只有 1 个 IP 地址（外部接口 IP 地址）的内部全局地址池
Router(config)#access-list 11 permit 192.168.1.0 0.0.0.255
//配置允许地址转换的内部本地地址范围
Router(config)#ip nat inside source list 11 pool abc overload
//配置内部本地地址与内部全局地址的映射关系。注意必须有 overload
Router(config)#interface FastEthernet 0/0                    //进入接口 f0/0 配置
Router(config-if)#ip address 192.168.1.1 255.255.255.0       //配置接口 f0/0 的 IP 地址
Router(config-if)#ip nat inside                              //配置接口 f0/0 为内部接口
Router(config-if)#no shutdown                                //启动接口
Router(config-if)#interface Serial 0/0                       //进入接口 s0/0 配置
Router(config-if)#ip address 220.123.10.1 255.255.255.0      //配置接口 s0/0 的 IP 地址
```

```
Router(config-if)#ip nat outside                          //配置接口 s0/0 为外部接口
Router(config-if)#no shutdown                             //启动接口
Router(config-if)#exit                                    //退出接口配置模式，回到全配置模式
Router(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0        //默认路由
Router(config)#end                                        //回到特权 EXEC 模式
```

6.5.6 访问控制列表配置

在路由器上，可通过使用访问控制列表（Access Control Lists，ACL）来执行数据包过滤。数据包过滤用来控制跨越网络的数据流。通过实现它，可以限制网络通信量，限制网络访问到特定的用户和设备。ACL 可用来控制网络上数据包的传递，限制虚拟终端线路的通信量或者控制路由选择更新。本节介绍访问控制列表及其基本配置。

1．访问控制列表概述

1）什么是访问控制列表

访问控制列表（ACL）是由一系列语句组成的列表，这些语句主要包括匹配条件和采取的动作（允许或禁止）两项内容。访问控制列表应用到路由器的接口上，通过匹配数据包信息与访问控制列表参数决定允许数据包通过还是拒绝数据包通过某个接口。数据包是通过还是拒绝，主要取决于通过数据包中的源地址、目的地址、源端口、目的端口、协议等信息。

建立 ACL 的原因很多，ACL 可以用来：

① 限制网络流量，提高网络性能。

② 提供流量控制。

③ 提供网络访问的基本安全级别。

④ 在路由器接口决定哪种流量被转发或被阻塞。

在路由器的接口上配置访问 ACL 后，可以对进出接口及通过接口中继的数据包进行安全检测。

2）访问控制列表分类

有三种基本的 IP 访问列表：标准型、扩展型和动态扩展型。

（1）标准型访问控制列表：以源 IP 地址寻址作为使用规则，提供了基本的过滤格式。

（2）扩展型访问控制列表：同时使用源地址和目标地址作为过滤，甚至允许用协议类型来过滤。

（3）动态扩展型访问控制列表：通过认证过程对每个用户确定对目标的访问权。

3）ACL 术语

（1）ACL 号码。ACL 要在全局配置模式中创建。有很多类型的 ACL，包括标准、扩展、IPX、AppleTalk 等。在路由器上配置 ACL 时，每个 ACL 必须通过为其分配一个号来惟一标志它。表 6.9 给出 ACL 的号码范围，号码的大小由用户正在应用的访问控制列表的设备来决定。

表 6.9　ACL 的号码范围

协　　议	范　　围
IP	1～99
扩展 IP	100～199

续表

协　　议	范　　围
Ethernet 类型码	200～299
DECnet	300～399
XNS	400～499
扩展 XNS	500～599
AppleTalk	600～699
Ethernet 地址	700～799
IPX	800～899
扩展 IPX	900～999
IPX SAP	1000～1099

（2）通配符掩码。访问控制列表的通配符掩码的作用与子网掩码类似，与 IP 地址一起使用，以确定某个主要网段上的所有主机。通配符掩码也是 32 位二进制数，与子网掩码相反，它的高位是连续的 0，低位是连续的 1，使用点分十进制来表示。表 6.10 是常用访问控制列表的通配符掩码示例。

表 6.10　常用访问控制列表的通配符掩码示例

通配符掩码	掩码的二进制形式	描　　述
0.0.0.0	00000000.00000000.00000000.00000000	整个 IP 地址必须匹配
0.0.0.255	00000000.00000000.00000000.11111111	只有前 24 位需要匹配
0.0.255.255	00000000.00000000.11111111.11111111	只有前 16 位需要匹配
0.255.255.255	00000000.11111111.11111111.11111111	只有前 8 位需要匹配
255.255.255.255	11111111.11111111.11111111.11111111	全部不需要匹配
0.0.15.255	00000000.00000000.00001111.11111111	只有前 20 位需要匹配
0.0.3.255	00000000.00000000.00000011.11111111	只有前 22 位需要匹配

IP 地址与通配符掩码的作用规则是：32 位的 IP 地址与 32 位的通配符掩码逐位进行比较，通配符掩码为 0 的位要求 IP 地址的对应位必须匹配，通配符掩码为 1 的位所对应的 IP 地址位不必匹配，例如：

IP 地址　　192.168.100.0（二进制为 11000000 10101000 01100100 00000000）

通配符掩码　0.0.0.255　　（二进制为 00000000 00000000 00000000 11111111）

该通配符掩码的前 24 位为 0，对应的 IP 地址位必须匹配，即必须保持原数不变，该通配符掩码的后 8 位为 1，对应的 IP 地址位不必匹配，即 IP 地址和后 8 位可以为任意值。也就是说，IP 地址“192.168.100.0”和通配符掩码“0.0.0.255”匹配的结果只有 192.168.100.0～192.168.100.255（共 256 个 IP 地址）是匹配的。

有两个特殊的通配符：一个是 host，另一个是 any。

host 表示一种精确匹配，是通配符掩码 0.0.0.0 的简写形式。例如，只检查 IP 地址为 172.16.100.10 的数据包，可使用以下两种 ACL 语句：

```
        access-list permit 172.16.100.10 0.0.0.0
或      access-list permit host 172.16.100.10
```

any 表示全部不进行匹配，是通配符掩码 255.255.255.255 的简写形式。例如，允许所有

的 IP 地址的数据都通过，可使用以下两种 ACL 语句：

```
        access-list permit 172.16.100.10 255.255.255.255
或      access-list permit any
```

2．配置ACL的基本步骤

一般来说，配置 ACL 需要下列两个基本步骤：

（1）创建访问控制列表。进入全局配置模式，使用 access-list 命令输入访问列表语句，确定列表类型号，后面跟上正确的参数。

（2）将访问控制列表应用到某一个接口。在接口配置模式下，使用 ip access-group 命令将 ACL 应用到一个或多个接口上，根据配置和如何被应用来过滤入站或出站流量。出站 ACL 通常比入站 ACL 要高效，因此优先选用出站 ACL。带有入站 ACL 的路由器在把分组交换到出站接口前，必须检查每一个分组是否与 ACL 条件判断语句相匹配。

3．配置标准ACL

配置标准 ACL 命令的详细语法如下：

```
access-list access-list-number {deny | permit} source [source-wildcard] [log]
```

表 6.11 列出了标准 ACL 命令中的参数与描述。

表 6.11　标准 ACL 命令中的参数与描述

参　数	描　述
access-list-number	访问列表编号。是一个 1～99 或 1300～1999 的十进制数字
deny	在匹配条件语句时，拒绝分组通过
permit	在匹配条件语句时，允许分组通过
source	发送分组的源地址，可以是网络地址或主机地址
source-wildcard	（可选项）通配符掩码用来与源地址一起使用
log	（可选项）生成有关分组匹配情况的日志消息，发送到控制台

使用标准版本的全局配置命令 access-list 来定义一个标准的 ACL，并给它分配一个数字编号，其编号范围为 1～99。

4．应用ACL到相应接口

```
ip access-group access-list-number {in | out}
```

应用 ACL 到某个接口时，必须指明其方向。in 表示通过接口进入路由器的报文，out 表示通过接口离开路由器的报文。

5．检验ACL

```
show access-list [access-list-number]          //显示所有协议的访问控制列表配置细节
show ip access-list [access-list-number]       //显示与 IP 协议有关的访问控制列表配置细节
```

6．标准ACL的配置实例

在如图 6.21 所示的网络中，要求配置 ACL，达到如下要求：PC1 不能访问 Server1 和 Server2，其他主机可以访问 Server1 和 Server2。

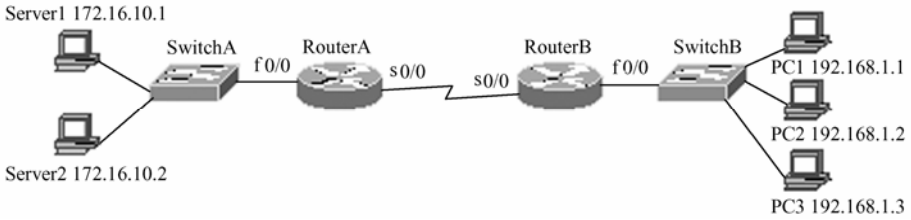


图 6.21　标准 IP 访问列表的配置

RouterB 的 ACL 配置如下：

```
RouterB#configure terminal                              //进入全局配置模式
RouterB(config)#access-list 10 deny host 192.168.1.1    //过滤 PC1 的所有报文
RouterB(config)#access-list 10 permit any               //允许其他主机的所有报文通过
RouterB(config)#interface f0/0                          //进入 f0/0 接口的配置
RouterB(config)#ip access-group 10 in                   //应用访问控制列表
```

由于 PC1 要与服务器通信必须经过 RouterB 的 f0/0 接口，因此只需要在 RouterB 上的 f0/0 接口应用访问控制列表就可达到目的。

本 章 小 结

本章主要介绍了以下内容。

（1）广域网是指覆盖范围广、传输速率相对较低、以数据传输为主要目的的数据通信网。广域网的结构分为通信子网与资源子网。广域网可以分为公共传输网络、专用传输网络和无线传输网络。

（2）PSTN 是以模拟技术为基础的电路交换网络。两个数字站通信时，要借助于 MODEM 实现。程控交换机是 PSTN 的核心设备。

（3）ISDN 是对模拟音频电话系统（PSTN）的再设计，它将决定用户设备与全局网络的连接，能方便地用数字的形式来处理声音、传真、影像和图像通信。ISDN 具有多种功能，包括电路交换、分组交换、无交换连接和公共信道信令功能等。B-ISDN 是一个高速、异步、时分、复用的综合业务数字网，它在各方面均比 ISDN 有了改进和加强。

（4）公共分组交换数据网是一种采用分组交换技术的数据通信网。分组交换采用存储/转发交换技术，分组是交换处理和传送的对象。分组交换数据网提供数据报和虚电路两类服务。X.25 协议是关于公用数据网上以分组方式工作的 DTE 和 DCE 之间的接口标准。

（5）帧中继是一种数据包交换技术，是 X.25 的简化版本。它运行在 OSI 参考模型的物理层和数据链路层。帧中继技术提供面向连接的数据链路层的通信。

（6）数字数据网（DDN）是利用数字信道提供永久或半永久性连接、传输数字信号的数字传输网络。DDN 由网络设备、连接电路和网络拓扑组成。

（7）网络互连是指将不同的网络连接起来，以构成更大规模的网络系统，实现网络间的数据通信和资源共享。网络互连可分为 LAN-LAN、LAN-WAN、LAN-WAN-LAN、WAN-WAN 四种类型。

（8）IP 地址是按照 IP 规定的格式，为每一个正式接入 Internet 的主机所分配的、供全世界标志的惟一通信地址。IP 分为 A、B、C、D、E 共 5 类，采用“点分十进制记法”。

（9）在实际应用中，需要对 IP 地址中的主机号部分进行再次划分，将其划分成子网号和主机号两部分，从而把一个包含大量主机的网络划分成许多小的网络，每个小网络就是一个子网。

（10）根据网络互连设备工作的层次及其所支持的协议，可以将网间设备分为中继器、网桥（或二层交换机）、路由器（或三层交换机）和网关。中继器用于物理层互连，网桥（或二层交换机）用于数据链路层互连，路由器（或三层交换机）用于网络层互连，网关用于网络层以上互连。

（11）Cisco 交换机所使用的操作系统是 IOS 或 COS。交换机可以通过 Console 端口、Telnet、浏览器、网管软件等来配置。Cisco IOS 提供三种基本的访问模式：用户 EXEC 模式、特权 EXEC 模式和配置模式。

（12）交换机的基本配置包括主机名和密码、交换机的管理 IP 地址和默认网关、管理 MAC 地址表、交换机端口、VLAN 等。常用命令有 hostname、password、enable password、interface、ip address、show 等。

（13）路由器的主要功能是，为经过路由器的每一个数据包寻找一条最佳通信路径并将该数据有效地传送到目标节点。选择最佳通信路径是由路由策略（即路由算法）来实现的，路由策略实际上就是路由器中保存的供路由选择时使用的各种传输路径的相关数据（路由表），路由表分为静态路由表和动态路由表。

（14）典型的路由选择方式有静态路由和动态路由。根据是否在一个自治系统内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。常用的内部网关协议有 RIP、OSPF，常用的外部网关协议是 BGP 和 BGP-4。

（15）路由器的基本配置包括主机名、系统时间和日期、各种接口以及口令设置，广域网 PPP、X.25、帧中继协议配置，静态路由和动态路由 RIP、OSPF 配置等。

（16）NAT 网络地址转换可以分为静态地址转换、动态地址转换、端口地址转换。

（17）可通过使用访问控制列表（ACL）在路由器上执行数据包过滤。ACL 分为标准型、扩展型和动态扩展型。配置 ACL 由创建 ACL 和将 ACL 应用到接口这两个基本步骤完成。

思 考 题

1．广域网与局域网的区别是什么？

2．常用的公共传输网络有哪些？

3．简述 PSTN 的组成。

4．什么是 ISDN？ISDN 定义了哪些接口速率？

5．什么是分组交换？为什么把公共分组交换数据网称为 X.25 网？

6．试述帧中继的组成及应用。

7．什么是 DDN？它有什么特点？

8．什么是 IP 地址？A、B、C 这 3 类地址是如何划分的？

9．为什么要进行子网划分？如何划分子网？

10．简述子网掩码和默认网关的作用。

11．Cisco IOS 有哪些命令模式？

12．在以下描述中，不正确的是（　　）。

A．设置了交换机的管理 IP 地址后，就可以使用 Telnet 方式来登录连接交换机，并实现对交换机的配置和管理

B．首次配置交换机时，必须采用 Console 端口

C．在默认情况下，交换机的所有端口都属于 VLAN1

D．交换机允许同时建立多个 Telnet 登录连接

13．在以下配置命令中，无法在用户 EXEC 模式下运行的是（　　）。

A．hostname　　B．show　　C．config t　　D．dir

14．试写出设置交换机的快速以太网端口 1～5 为 100M 全双工通信方式的配置命令。

15．什么是 VLAN？划分 VLAN 的方法有哪些？

16．要将一台 Cisco 2950 交换机划分为 4 个 VLAN，每个 VLAN 中均包含 6 个端口，应该如何进行配置？

17．在模拟软件 Boson netsim 中练习交换机的配置。

18．在路由器的初始化配置或 setup 过程中，哪个组合键可以用于退出该过程？（　　）

A．Ctrl+A　　B．Ctrl+E　　C．Ctrl+C　　D．Ctrl+D

19．如果计划配置一个接口，路由器应该处于哪个提示符？（　　）

A．Router(config)#　　B．Router(config-in)#

C．Router(config-intf)#　　D．Router(config-if)#

20．在提示符为 Router(config-if)#的配置模式下，exit 命令的作用是什么？（　　）

A．退出当前的接口配置模式

B．到达特权 EXEC 模式

C．退出路由器

D．切换到用户 EXEC 模式

21．从配置模式进入线路配置模式的命令是什么？（　　）

A．Router(config)#line con 0 4

B．Router(config)#interface line vty 0 4

C．Router(config)#interface line con 0 4

D．Router(config)#line vty 0 4

22．下面哪一项不是 Cisco IOS show version 命令显示的信息？（　　）

A．配置接口的统计信息

B．Cisco IOS 软件运行的平台类型

C．配置寄存器的设置

D．Cisco IOS 软件版本

23．动态路由协议与静态路由协议有什么不同？常用的动态路由协议有哪些？

24．哪一项最好地描述了默认路由？（　　）

A．网络管理员手工输入的紧急数据路由

B．当网络的一部分出现故障时使用的路由

C．当目的网络没有明确列在路由选择表中时使用

D．预先设置的最短路径

25．配置静态路由的命令是哪一条？（　　）

A．Router(config)#ip router 192.168.1.0 255.255.255.0 serial 0/0

B．Router(config)#ip router 192.168.1.0 255.255.255.0

C．Router#ip router 192.168.1.0 255.255.255.0 serial 0/0

D．Router(config-if)#ip router 192.168.1.0 255.255.255.0 serial 0/0

26．查看路由表的命令是哪一条？（　　）

A．Router#show ip routing　　B．Router#show ip router

C．Router#show ip route　　D．Router#show ip-route

27．RIP 使用下面哪个度量标准来确定数据传输的最佳路径？（　　）

A．带宽　　B．跳数

C．根据传输的数据不同而变化　　D．管理距离

28．如果想知道路由器配置了哪些路由协议，应该使用什么命令？

29．什么是 ACL？ACL 的功能是什么？ACL 是如何分类的？

30．在进行 ACL 配置时应注意哪些问题？

31．命令 access-list 10 permit 204.11.19.162 0.0.0.0 可以实现以下哪种功能？（　　）

A．只拒绝本网段地址　　B．允许一个指定的主机

C．只允许本网通过　　D．以上都不是

32．什么是 NAT？NAT 分为哪几类？

实训 8　交换机的配置与管理

一、实训目的

1．了解交换机的启动过程，掌握交换机的配置途径。

2．对交换机进行基本设置。

3．熟悉和掌握对交换机的端口配置和查看端口信息。

4．掌握静态 MAC 地址的配置方法和 MAC 地址表的查看方法。

二、实训设备

1．1 台 Cisco Catalyst2950 系列交换机。

2．1 台 PC，运行 Windows 操作系统，装有超级终端程序。

3．控制线 1 根，T568B 标准的网线 1 根。

三、实训内容

1．连接交换机与 PC。将控制线的 RJ-45 插头插入交换机的 Console 端口，DB-9 插头插入计算机的串口 COM1 或 COM2。

2．配置超级终端。在 Windows 中启动超级终端程序，并创建一个名为 Switch 的新连接，设置好 COM 端口的属性。

3．接通交换机的电源，在超级终端中观察交换机的启动过程信息。若交换机还不曾配置过，在启动时，将询问是否要进行初始配置，可选择“N”跳过或选择“Y”，再按配置向导的提示，对交换机进行基本配置。

4．启动成功后，在交换机上练习如下命令：?、enable、show run、show version。

5．配置交换机的主机名为 Cisco2950，并设置管理 IP 为 192.168.10.10，配置进入特权 EXEC 模式的密码为 cisco-en，配置 vty 0～5 条线路的登录密码为 cisco-vty，配置 Console 的登录密码为 cisco-con，用 show run 查看当前配置，然后用 copy run start 保存配置到 NVRAM。

6．执行 reload 命令重新启动交换机，进入用户 EXEC 模式时需要 console 登录密码，键入在第 5 步中设置的 console 密码进入用户 EXEC 模式；再键入 enable 进入特权 EXEC 时也要输入特权密码。

7．通过 telnet 登录交换机。将 PC 网卡用网线接入到交换机的任一快速以太网端口上（假设为 f0/5），再将 PC 的 IP 地址设置为 192.168.10.100，然后进入 Windows 的 DOS 命令提示符方式，键入 telnet 192.168.10.10 登录交换机。

8．在超级终端中对交换机进行配置，进入接口配置模式，执行 shutdown 命令关闭端口 f0/5，观察交换机的 5 号端口指示灯的变化、计算机的网络连接状态的变化，执行 show int f0/5 查看端口的状态。然后执行 no shutdown，再观察端口指示灯的变化，再执行 show int f0/5 查看端口的状态。

实训 9　VLAN 的配置与管理

一、实训目的

1．熟悉和掌握 VLAN 配置。

2．掌握 VTP 的配置方法和命令。

3．熟悉通过 VLAN Trunk 配置跨交换机的 VLAN。

4．掌握查看 VLAN、VTP 及 VLAN Trunk 的命令。

二、实训设备

1．2 台 Cisco Catalyst2950 系列交换机。

2．4 台 PC，运行 Windows 操作系统，装有超级终端程序。

3．控制线 2 根，T568B 标准的网线 3 根，交叉网线 1 根。

三、实训要求

实训拓扑图如图 6.22 所示，用交叉网线连接 SwitchA 的 f0/1 与 SwitchB 的 f0/1 端口。4 台 PC 网卡分别用直通线连入对应交换机的端口。

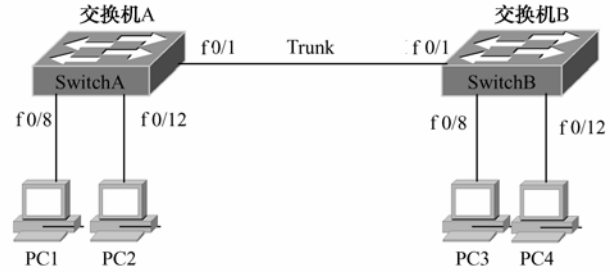


图 6.22　VLAN 配置与管理实训拓扑图

四、实训内容

1．按图 6.22 所示连接好网络，并配置交换机 A 和交换机 B 的主机名分别为 SwitchA 和 SwitchB。

2．将设置 PC1、PC2、PC3 和 PC4 的 IP 地址分别为 192.168.10.10、192.168.10.20、192.168.10.30 和 192.168.10.40，网关地址为 192.168.10.254。

3．在 PC1 中，分别 ping PC2、PC3、PC4，全都能 ping 通。

4．在 SwitchA 上创建 VLAN2，将 SwitchA 的 f0/9～f0/12 划入 VLAN2，f0/13～f0/16 划入 VLAN3，用 show vlan 命令查看划分结果。

5．在 PC1 中，ping 各 PC，检查同一 VLAN 内和不同 VLAN 间各主机能否相互通信。PC1 到 PC3 和 PC4 通，而到 PC2 不通。为什么？

6．将 SwitchA 配置成 VTP Server，SwitchB 配置成 VTP Client，域名为 CEC。验证 VTP 配置。

7．将 SwitchA 和 SwithB 的 f0/1 端口均配置成 Trunk 端口。

8．在 SwitchB 上用 show vlan 查看是否从 SwitchA 上得到有关的 VLAN 的设置信息。此时，SwitchB 上的 VLAN 信息应与 Switch 相同。

9．再次在 PC1 中，ping 各 PC，此时 PC1 到 PC3 通，到 PC2 和 PC4 不通。为什么？

实训 10　路由器的基本配置

一、实训目的

1．熟悉路由器的基本配置方法。

2．掌握主机名、系统时钟、密码、远程登录、默认路由的配置。

3．掌握路由器 LAN 接口和 WAN 接口的配置命令和方法。

二、实训环境

1．PC1 台，运行 Windows 操作系统，装有超级终端程序。

2．Cisco 2611 路由器 1 台。

3．WIC-1T 模块 1 个。

4．V.35 DTE 电缆 1 根，V.35 DCE 电缆 1 根，交叉网线 1 根。

5．Console 控制线 1 根。

三、实训内容

1．正确连接路由器的 Console 线和电源线。

2．启动超级终端连接，打开路由器的电源，熟悉路由器的启动信息。

3．配置路由器的主机名、系统时钟、enable 密文密码。

4．配置 Serial 端口的描述、IP 地址、线路速率、连接线路的带宽、封装协议类型、打开接口。

5．配置 FastEthernet 端口的描述、IP 地址、打开接口。

实训 11　路由协议的配置与管理

一、实训目的

1．掌握静态路由的配置。

2．掌握 RIP（路由选择信息协议）的基本配置与验证。

3．掌握 OSPF（开放最短路径优先）协议的基本配置。

二、实训参数及网络拓扑结构

路由协议配置实训网络拓扑图如图 6.23 所示。

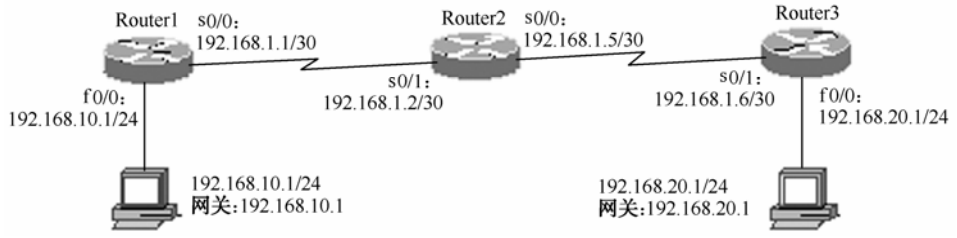


图 6.23　路由协议配置实训网络拓扑图

三、实训设备

1．PC2 台，运行 Windows 操作系统，装有超级终端程序。

2．Cisco 2611XM 路由器 3 台。

3．WIC-1T 模块 4 个。

4．V.35 DTE 电缆 2 根，V.35 DCE 电缆 2 根，交叉网线 2 根。

5．Console 控制线 3 根。

四、实训内容

1．通过对静态路由协议的配置，实现全网的连通。

2．通过对 RIP 路由选择协议的配置，实现全网的连通。

3．声明相应网络进入 RIP 路由进程。

4．查看路由表并理解相关字段含义。

5．监测 RIP 协议的路由更新发送和接收情况等相关信息。

6．去除 RIP 协议，在路由器上启动和配置 OSPF 协议。

7．声明相应网络进入 OSPF 路由信息。

8．查看 OSPF 协议的配置、邻居、接口和路由等信息。

实训 12　配置PPP和X.25 协议

一、实训目的

1．掌握 PPP（点到点协议）的基本配置与验证。

2．掌握 X.25 协议的基本配置与验证。

二、实训参数及网络拓扑结构

配置参数和网络拓扑结构如图 6.24 所示。

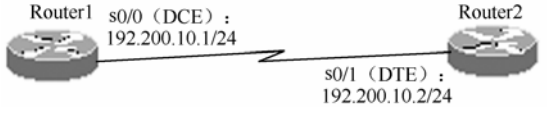


图 6.24　配置参数和网络拓扑结构

三、实训设备

1．PC1 台，运行 Windows 操作系统，装有超级终端程序。

2．准备 Cisco 2611XM 路由器 2 台，分别为 Router1 和 Router2。

3．WIC-1T 模块 2 个。

4．DTE 电缆 1 根，DCE 电缆 1 根。

5．Console 控制线 2 根。

四、实训内容

1．PPP 的两种验证方式（CHAP 和 PAP）的配置。

2．X.25 协议的基本配置与验证。

3．查看接口及 X.25 相关信息。

实训 13　配置帧中继协议

一、实训目的

1．配置普通路由器 Router1 作为帧中继交换机使用，以便为基本的帧中继实训提供帧中继交换机的实训环境。

2．掌握配置帧中继，实现网络互连。

二、实训参数及网络拓扑结构

帧中继配置参数和网络拓扑结构如图 6.25 所示。

三、实训设备

1．PC2 台，运行 Windows 操作系统，装有超级终端程序。

2．Cisco 2611XM 路由器 3 台，分别为 Router1、Router2 和 Router3。

3．WIC-1T 模块 4 个。

4．交叉网线 2 根，V.35 DCE 电缆 2 根，V.35 DTE 电缆 2 根。

5．Console 控制线 2 根。

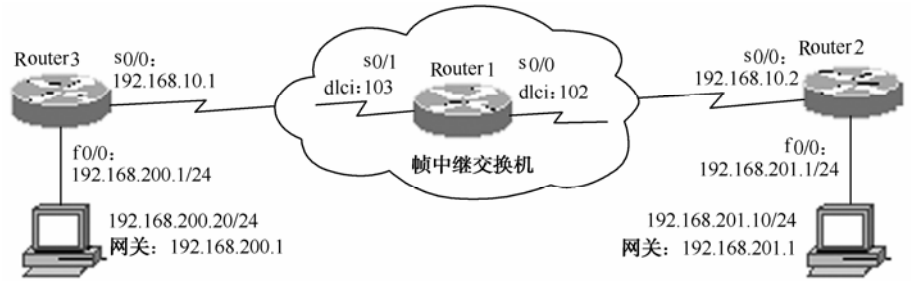


图 6.25　帧中继配置参数和网络拓扑结构

四、实训内容

1．配置普通路由器 Router1 作为帧中继交换机使用。

2．基本的帧中继配置，实现网络互连。

3．查看和监测帧中继相关信息。

4．查看帧中继 PVC 通信状态信息。

实训 14　NAT配置与管理

一、实训目的

1．从实训角度理解、配置和监测 NAT。

2．掌握配置静态地址转换（NAT）。

3．掌握 PAT 配置。

二、实训参数及网络拓扑结构

NAT 配置参数和网络拓扑结构如图 6.26 所示。

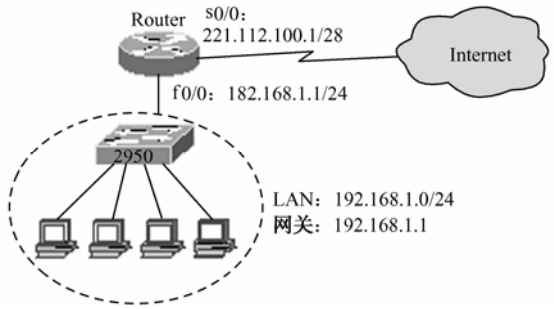


图 6.26　NAT 配置参数和网络拓扑结构

三、实训设备

1．PC 若干台，运行 Windows 操作系统，装有超级终端程序。

2．Cisco 2611 路由器 1 台，Cisco 2950 交换机 1 台。

3．WIC-1T 模块 2 个。

4．直通网线若干，DTE 电缆 1 根，DCE 电缆 1 根。

5．Console 控制线 1 根。

四、实训内容

1．在 Router 上配置静态 NAT 和 PAT。

2．在 Router 上配置 PAT。

3．查看 NAT 的相关信息。

4．监测 IP 地址的转换。

5．测试内网和外网间的双向连通性。

第 7 章　Internet接入技术

本章要点

本章从 Internet 接入技术的概念入手，介绍常用的接入技术，RAS 的配置，Intranet 的概念、技术及网络组成。

本章目标

- 了解 Internet 接入技术的概念
- 了解常用的接入技术
- 掌握 ADSL 接入方法
- 了解 RAS 的配置方法
- 了解 Intranet 的概念、技术要点和网络组成

用户计算机和用户网络接入 Internet 所采用的技术和接入方式的结构，统称为 Internet 接入技术，又称最后一公里技术（Last Mile Technology），其发生在连接网络与用户的最后一段路程，是网络中技术最复杂、实施最困难、影响面最广的一部分。

关于 Internet 接入技术，除了需要掌握接入网外，还需要了解 ISP 和骨干网。

1．Internet接入网

Internet 接入网分为主干系统、配线系统和引入线三个部分。其中，主干系统为传统电缆和光缆，一般长度为数公里；配线系统也可能是电缆或光缆，长度一般为几百米；引入线通常为几米到几十米，多采用铜线。接入网根据使用的介质可以分为有线接入网和无线接入网两大类，其中有线接入网又可分为铜线接入网、光纤接入网和光纤同轴电缆混合接入网等，无线接入网又可分为固定接入网和移动接入网。

2．ISP

ISP（Internet Service Provider，Internet 服务提供商）是指为用户提供 Internet 接入和 Internet 信息服务的公司和机构。根据服务的侧重点不同，ISP 可分为两种：IAP（Internet Access Provider）和 ICP（Internet Content Provider）。IAP 是 Internet 接入提供商，以接入服务为主；ICP 是 Internet 内容提供商，以提供信息服务为主。用户的计算机（或网络）通过某种通信线路连接到 ISP，借助于与国家骨干网相连的 ISP 接入 Internet。从某种意义上讲，ISP 是全世界数以亿计的用户通往 Internet 的必经之路。

3．骨干网

骨干网是国家批准的可以直接和国外连接的城市级高速互联网，它由所有用户共享，负责传输大范围（在城市之间和国家之间）的骨干数据流。骨干网基于光纤，通常采用高速传输网络传输数据和高速包交换设备提供网络路由。建设、维护和运营骨干网的公司或单位称为 Internet 运营机构（也称为 Internet 供应商）。不同的 Internet 运营机构拥有各自的骨干网。国内各种用户想连到国外网都必须通过这些骨干网。我国现有的 Internet 骨干网主要有：中国

公用计算机互联网（CHINANET）、中国教育和科研计算机网（CERNET）、中国联通计算机互联网（UNINET）、中国科技网（CSTNET）、中国网通公用互联网（CNCNET）、中国移动互联网（CMNET）和中国卫星集团互联网（CSNET）等。

7.1 常用的接入技术

Internet 接入技术很多，除了最常见的拨号接入外，还有目前正广泛应用的宽带接入。宽带接入相对于传统的窄带接入而言显示了其不可比拟的优势和强劲的生命力。宽带是一个相对于窄带而言的电信术语，为动态指标，用于度量用户享用的业务带宽，目前国际还没有统一的定义，一般而论，宽带是指用户接入传输速率达到 1Mbps 及以上、可以提供 24h 在线的网络基础设备和服务。宽带接入技术主要包括以现有电话网铜线为基础的 xDSL 接入技术，以电缆电视为基础的混合光纤同轴（HFC）接入技术，以太网接入、光纤接入技术等多种有线接入技术以及无线接入技术。

7.1.1 电话拨号接入

电话拨号接入是个人用户接入 Internet 的最早使用的方式之一，也是到目前为止我国个人用户接入 Internet 使用得最广泛的方式之一，它将用户计算机通过电话网接入 Internet。

电话拨号接入非常简单，只需一个调制解调器（MODEM）、一根电话线即可，但速度很慢，理论上只能提供上行 33.6kbps 和下行 56kbps 的速率，主要用于个人用户。拨号上网多采用“点到点协议”（Point to Point Protocol，PPP），使用调制解调器，通过电话网与 ISP 主机连接，再通过 ISP 的路由器接入 Internet。这种方式的优点是，用户上网时拥有独立的 IP 地址，与 Internet 上其他主机的地位是平等的。另外，由于动态分配 IP 地址，可充分利用有限的 IP 地址资源，并且降低了每个用户的入网费用。

7.1.2 xDSL接入

xDSL 是 DSL（Digital Subscriber Line，数字用户线）的统称，是以电话铜线（普通电话线）为传输介质、点对点传输的宽带接入技术。它可以在一根铜线上分别传送数据和语音信号，其中数据信号并不通过电话交换设备，并且不需要拨号，不影响通话。xDSL 的最大优势在于利用现有的电话网络架构，不需要对现有接入系统进行改造，就可方便地开通宽带业务，被认为是解决“最后一公里”问题的最佳选择之一。

xDSL 同样是调制解调技术家族的成员，只是采用了不同于普通 MODEM 的标准，运用先进的调制解调技术，使得通信速率大幅度提高，最高能够提供比普通 MODEM 快 300 倍的兆级传输速率。此外，与电话拨号方式不同的是，xDSL 只利用电话网的用户环路，并非整个网络，采用 xDSL 技术调制的数据信号实际上是在原有话音线路上叠加传输，在电信局和用户端分别进行合成和分解，为此，需要配置相应的局端设备。常用的 xDSL 技术如表 7.1 所示。

表 7.1 常用的 xDSL 技术

XDSL	名　　称	对 称 性	下行速率（bps）	上行速率（bps）	极限传输距离（km）
IDSL	ISDN 数字用户线	对称	128k	128 k	4.6~5.5
SDSL	单线路数字用户线	对称	1.5M	1.5M	3
HDSL（2 对线）	高速率数字用户线	对称	1.544~2M	1.544~2M	2.7~3.6

续表

XDSL	名　　称	对 称 性	下行速率（bps）	上行速率（bps）	极限传输距离（km）
ADSL	非对称数字用户线	非对称	1.544～8.192M	512k～1M	2.7～3.6
VDSL	甚高速数字用户线	非对称	12.96～55.2M	1.5～2.3M	0.3～1.4

在表 7.1 中，xDSL 技术分为对称和非对称技术两种模式。对称 DSL 技术指上、下行双向传输速率相同的 DSL 技术，方式有 IDSL、SDSL、HDSL 等，主要用于替代传统的 T1/E1 接入技术。这种技术具有对线路质量要求低、安装调试简单的特点。非对称 DSL 技术为上、下行传输速率不同，上行较慢，下行较快的 DSL 技术，主要有 ADSL、VDSL 等，适用于对双向带宽要求不一样的应用，如 Web 浏览、多媒体点播、信息发布、视频点播 VOD 等，是 Internet 接入中很重要的一种方式，目前最常用的是 ADSL 技术。

ADSL（Asymmetrical Digital Subscriber Line，非对称数字用户线）是在无中继的用户环路上，使用由负载电话线提供高速数字接入的传输技术，是非对称 xDSL 技术的一种，可在现有电话线上传输数据，误码率低。ADSL 技术为家庭和小型业务提供了宽带、高速接入 Internet 的方式。在普通电话双绞线上，ADSL 的典型上行速率为 512kbps～1Mbps，下行速率为 1.544～8.192Mbps，传输距离为 2.7～3.6km。

一个基本的 ADSL 系统由局端收发机和用户端收发机两部分组成，收发机实际上是一种高速调制解调器——ADSL MODEM，由其产生上、下行的不同速率。基于 ADSL 的接入网主要由数字用户线接入复用器（DSL Access Multiplexer，DSLAM）、用户线和用户家中的一些设施组成，如图 7.1 所示。

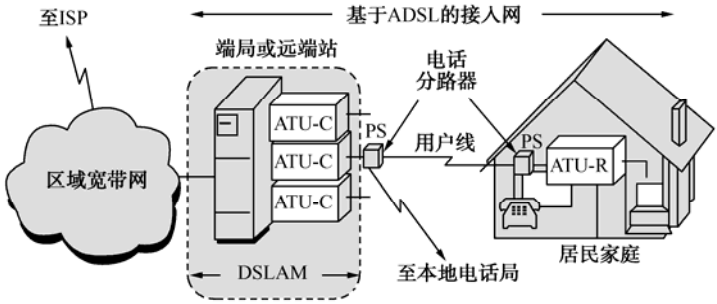


图 7.1　基于 ADSL 的接入网

数字用户线接入复用器包括许多 ADSL MODEM。ADSL MODEM 又称为接入端单元 ATU（Access Termination Unit）。由于 ADSL MODEM 必须成对使用，因此处于端局位置的 ADSL MODEM 称为 ATU-C（C 代表端局 Central Office）和 ATU-R（R 代表远端 Remote）。用户电话通过电话分线器（POTS Splitter，PS）和 ATU-R 连在一起，经用户线到端局，并经过一个电话分路器（PS）将电话连到本地电话交换机。电话分路器（PS）利用低通滤波器将电话信号与数字信号分开。

从客户端设备和用户数量来看，可以分为以下四种接入情况：

（1）单用户 ADSL MODEM 直接连接。此方式多为家庭用户使用，连接时用电话线将滤波器一端接于电话机上，一端接于 ADSL MODEM，再用交叉网线将 ADSL MODEM 和计算机网卡连接即可（如果使用 USB 接口的 ADSL MODEM，则不必用网线）。

（2）多用户 ADSL MODEM 连接。若有多台计算机，就先用集线器组成局域网，设其中

一台为服务器，并配以两块网卡，一块接 ADSL MODEM，另一块接集线器的 uplink 口（用直通网线）或 1 口（用交叉网线），滤波器的连接与（1）中相同。其他计算机即可通过此服务器接入 Internet。

（3）小型网络用户 ADSL 路由器直接连接计算机。客户端除使用 ADSL MODEM 外还可使用 ADSL 路由器，它兼具路由功能和 MODEM 功能，可与计算机直接相连，不过由于它提供的以太端口数量有限，因而只适合于用户数量不多的小型网络。

（4）大量用户 ADSL 路由器连接集线器。当网络用户数量较大时，可以先将所有计算机组成局域网，再将 ADSL 路由器与集线器或交换机相连，其中接集线器 uplink 口用直通网线，接集线器 1 口或交换机用交叉网线。

ADSL 的用途十分广泛，对于商业用户来说，可组建局域网共享 ADSL 上网，还可以实现远程办公、家庭办公等高速数据应用，获取高速低价的极高性价比。对于公益事业来说，ADSL 可以实现高速远程医疗、教学、视频会议的即时传送，达到以前所不能及的效果。

7.1.3 HFC接入

光纤同轴混合网（HFC 网）于 1988 年提出。从用户数量看，我国已拥有世界上最大的有线电视网，其覆盖率高于电话网。HFC 网就是在充分利用这一资源，改造原有线路，变单向信道为双向信道，实现高速接入 Internet 的思想推动下出现和发展起来的。

1．HFC概念

光纤同轴电缆混合网（Hybrid Fiber Coaxial，HFC）是一种新型的宽带网络，也可以说是有线电视网的延伸。HFC 接入技术是以有线电视网 CATV 为基础，采用模拟频分复用技术，综合应用模拟和数字传输技术、射频技术和计算机技术所产生的一种宽带接入网技术。以这种方式接入 Internet 可以实现 10～40Mbps 的带宽，用户可享受的平均速度是 200～500kbps，最快可达 1500kbps，用它可以非常舒心地享受宽带多媒体业务，并且可以绑定独立 IP。

2．HFC接入系统组成

HFC 网络中传输的信号是射频信号（Radio Frequency，RF），即一种高频交流变化电磁波信号，类似于电视信号，在有线电视网上传送。HFC 接入系统由三部分组成：前端系统、HFC 接入网和用户终端系统，如图 7.2 所示。

依据图 7.2 从上行和下行两条线路来看 HFC 系统中信号传送过程。

（1）下行方向。在前端，所有服务或信息经由相应调制转换成模拟射频信号，这些模拟射频信号和其他模拟音频、视频信号经数模混合器由频分复用方式合成一个宽带射频信号，加到前端的下行光发射机上，并调制成光信号用光纤传输到光节点并经同轴电缆网络、数模分离器和 Cable MODEM 将信号分离解调并传输到用户。

（2）上行方向。用户的上行信号采用多址技术（如 TDMA、FDMA、CDMA 或它们的组合）通过 Cable MODEM 复用到上行信道，由同轴电缆传送到光节点进行电光转换，然后经光纤传至前端，上行光接收机再将信号经分接器分离、CMTS 解调后传送到相应接收端。

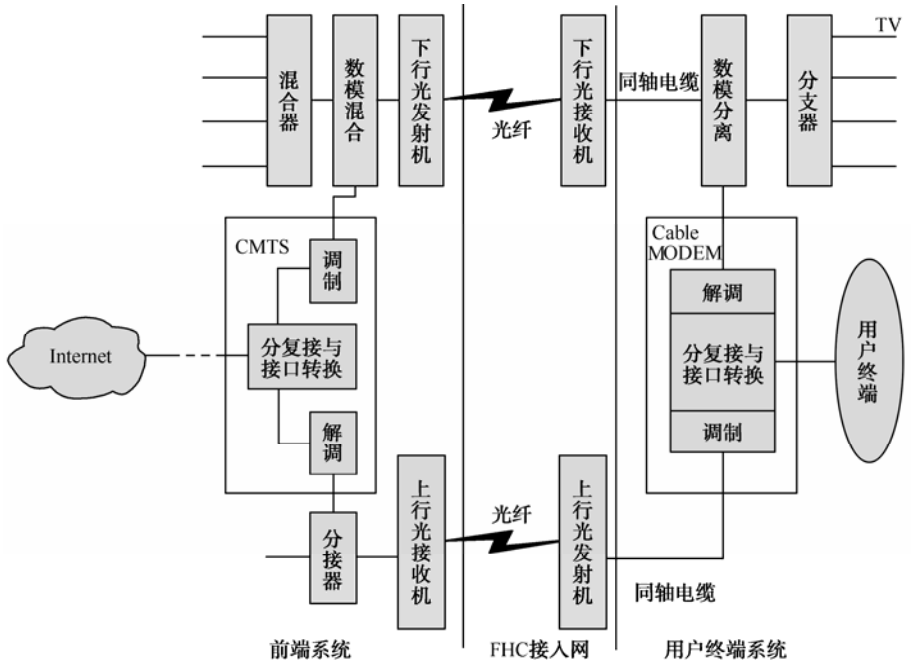


图 7.2　HFC 接入系统

3．HFC接入的主要特点

现有的 CATV 网是树形拓扑结构的同轴电缆网络，它采用频分复用技术对电视信号进行单向传输。HFC 网则需要对 CATV 网进行改造，其主要特点如下。

（1）HFC 网的主干线路采用光纤。

（2）HFC 网采用节点体系结构。这种体系结构的特点是：从头端到各个光纤节点用模拟光纤连接，构成星形网。光纤节点以下是同轴电缆组成的树形网。

（3）HFC 网具有比 CATV 网更宽的频谱，并且具有双向传输功能。

（4）每个家庭要安装一个用户接口盒。这个用户接口盒要提供三种连接：使用同轴电缆连接到机顶盒（Set Top Box，STB），然后再连接到用户的电视机；使用双绞线连接到用户的电话机；使用线缆调制解调器（Cable MODEM）连接到用户的计算机。

4．机顶盒

机顶盒（Set Top Box，STB）是一种扩展电视机功能的新型家用电器，由于常放在电视机顶上，所以称为机顶盒。目前的机顶盒多为网络机顶盒，其内部包含操作系统和互联网浏览软件，通过电话网或有线电视网连接互联网，使用电视机作为显示器，从而实现没有计算机的上网。

5．线缆调制解调器

线缆调制解调器（Cable MODEM）是为 HFC 网而使用的调制解调器。线缆调制解调器最大的特点就是传输速率高，其下行速率一般为 3～10Mbps，最高可达 30Mbps；而上行速率一般为 0.2～2Mbps，最高可达 10Mbps。然而，线缆调制解调器比在普通电话线上使用的调制解调器要复杂得多，并且不是成对使用，而是只安装在用户端。

7.1.4　光纤接入

光纤接入技术实际就是在接入网中全部或部分采用光纤传输介质，构成光纤用户环路（Fiber In The Loop，FITL），实现用户高性能宽带接入的一种方案。

光纤接入网（Optical Access Network，OAN）是指在接入网中用光纤作为主要传输介质来实现信息传输的网络形式，它不是传统意义上的光纤传输系统，而是针对接入网环境所专门设计的光纤传输网络。

1．光纤接入网的分类

从光纤接入网的网络结构看，按接入网室外传输设施中是否含有源设备，可以划分为有源光网络（Active Optical Network，AON）和无源光网络（Passive Optical Network，PON）。

（1）有源光网络（AON）。AON 指从局端设备到用户分配单元之间均使用有源光纤传输设备，如光电转换设备、有源光电器件、光纤等连接成的光网络。采用有源光节点可降低对光器件的要求，可应用性能低、价格便宜的光器件，但是初期投资较大，作为有源设备存在电磁信号干扰、雷击以及有源设备固有的维护问题，因而有源光纤接入网不是接入网的长远发展方向。

（2）无源光网络（PON）。PON 指从局端设备到用户分配单元之间不含有任何电子器件及电子电源，全部由光分路器等无源器件连接而成的光网络。由于它初期投资少、维护简单、易于扩展、结构灵活、大量的费用将在宽带业务开展后支出，因而目前光纤接入网几乎都采用此结构，它是光纤接入网的长远解决方案。

2．光纤接入方式

根据光网络单元（Optical Network Unit，ONU）所在位置，光纤接入网可以统称为 FTTx（即光纤到……），字母 x 可代表不同的意思（和 xDSL 中的字母 x 的作用相似）。光纤接入网的接入方式分为光纤到路边（Fiber To The Curb，FTTC）、光纤到大楼（Fiber To The Building，FTTB）、光纤到办公室（Fiber To The Office，FTTO）、光纤到楼层（Fiber To The Floor，FTTF）、光纤到小区（Fiber To The Zone，FTTZ）、光纤到户（Fiber To The Home，FTTH）等几种类型，其中 FTTH 是未来宽带接入网发展的最终形式。光纤接入方式如图 7.3 所示。

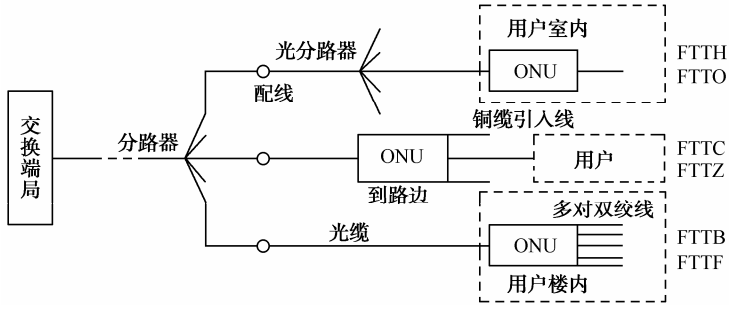


图 7.3　光纤接入方式

3．FTTx+LAN接入

FTTx+ LAN，即由光纤接入和以太网技术结合而成的高速以太网接入方式，可实现“千兆到楼，百兆到层面，十兆到桌面”，为最终光纤到户提供了一种过渡。FTTx+LAN 接入比较简单，在用户端通过一般的网络设备（如交换机、集线器等）将同一幢楼内的用户连成一个局域网，用户室内只需添加以太网 RJ-45 信息插座和配置以太网接口卡（即网卡）；在另一端

通过交换机与外界光纤干线相连即可。总体来看，FTTx+LAN 是一种比较廉价、高速、简便的数字宽带接入技术，特别适用于我国这种人口居住密集型的国家。

7.1.5 通过数据通信线路接入

1．DDN专线接入

对于上网计算机较多、业务量大的企业用户，可以采用租用电信专线的方式接入 Internet。广义上，专线接入是指通过 DDN、帧中继、X.25、数字专用线路、卫星专线等数据通信线路与 ISP 相连，借助 ISP 与 Internet 骨干网的连接通路访问 Internet 的接入方式。其中，DDN 专线接入最为常见，应用较广。

DDN 专线利用光纤、数字微波、卫星等数字信道和数字交叉复用节点，传输数据信号，可实现 2Mbps 以内的全透明数字传输以及高达 155Mbps 速率的语音、视频等多种业务。DDN 专线接入时，对于单用户通过市话模拟专线接入的，可采用调制解调器、数据终端单元设备和用户集中设备就近连接到电信部门提供的数字交叉连接复用设备处；对于用户网络接入就采用路由器、交换机等。DDN 专线接入特别适用于金融、证券、保险业、外资及合资企业、交通运输行业、政府机关等。

2．ISDN接入

ISDN（Integrated Services Digital Network，综合业务数字网）接入，俗称“一线通”，是普通电话（模拟 MODEM）拨号接入和宽带接入之间的过渡方式。目前，在我国只提供 N-ISDN（窄带综合业务数字网）接入业务，而基于 ATM 技术的 B-ISDN（宽带综合业务数字网）尚未开通。

ISDN 接入 Internet 与使用 MODEM 普通电话拨号方式类似，也有一个拨号的过程。不同的是，它不用 MODEM 而是用另一设备（ISDN 适配器）来拨号。另外，普通电话拨号在线路上传输模拟信号，有一个 MODEM“调制”和“解调”的过程；而 ISDN 的传输是纯数字过程，通信质量较高，其数据传输比特误码率比传统电话线路至少改善 10 倍。它的连接速度快，一般只需几秒即可拨通。ISDN 的最高数据传输速率可达 128kbps。

7.1.6 无线接入

各种研究报告表明，预计到 2010 年，全球移动用户数量将达到 45 亿人，将有 30 亿部移动设备接入 Internet。无线接入在众多的新兴接入技术中备受瞩目。

无线接入技术是指从业务节点到用户终端之间的全部或部分传输设施采用无线手段，向用户提供固定和移动接入服务的技术。采用无线通信技术将各用户终端接入到核心网的系统，或者是在市话端局或远端交换模块以下的用户网络部分采用无线通信技术的系统都统称为无线接入系统。由无线接入系统所构成的用户接入网称为无线接入网。无线接入是本地有线接入的延伸、补充或临时应急方式。

无线接入按接入方式和终端特征通常分为固定接入和移动接入两大类。

（1）固定无线接入，指从业务节点到固定用户终端采用无线技术的接入方式，用户终端不含或仅含有限的移动性。此方式是用户上网浏览及传输大量数据时的必然选择，主要包括卫星、微波（LMDS）、扩频微波、无线光传输和特高频。

（2）移动无线接入，指用户终端移动时的接入，包括移动蜂窝通信网（GSM、CDMA、TDMA、CDPD）、无线寻呼网、无绳电话网、集群电话网、卫星全球移动通信网以及个人通

信网等，是当前接入研究和应用中很活跃的一个领域。

7.1.7 电力线接入

电力线通信是使用低压民用电力线来传输网络数据的通信技术，电力线上网就是使用原有的低压 220V 电源线作为数据通信的线路载体；将原来所有电源插座变为信息插座而组建的网络称为电力线通信网络。

电力线接入 Internet 的技术，实际上就是计算机通过专用的网卡，接入到电源线，通过转换装置，将网络信号转换成电力线的信号，便可通过专用的网卡上网。

电力线通信是接入网的一种替代方案，因为与电话线、有线电视网相比，电力线的线路覆盖范围要小得多。在室内组网方面，计算机、打印机、电话和各种智能控制设备都可通过普通电源插座，由电力线连接起来，组成局域网。现有的各种网络应用：话音、电视、多媒体业务、远程教育等，都可通过电力线向用户提供，以实现接入和室内组网的多网合一。

电力线接入是未来发展的一大重要方向。电力网作为宽带接入介质，除了可以提供互联网接入的新选择外，还能够解决“最后一公里”问题，但目前技术方面还有待于进一步研究，各种相关问题也有待于进一步解决。

7.2 配置RAS并利用电话网接入

7.2.1 远程访问的概念

为了实现移动办公，即无论出差在外还是下班回家，职工希望随时登录到公司的网络中查看、下载资料，或者为客户提供登录网络查询业务数据服务。这就要求公司的网络允许用户通过拨号的方式登录访问，即提供远程访问服务（Remote Access Service，RAS）。

目前常用的远程访问方式有两种：远程遥控、远程客户端。

“远程遥控”是目前在 PC 上常见的一种远程访问方式，远程遥控软件有 PC Anywhere、Carbon Copy 等。“远程客户端”是 Windows 2000 的拨号网络所提供的方式，下面讨论如何在 Windows 2000 的网络中实现远程访问服务（RAS）。

一台安装了“路由和远程访问”的 Windows Server 2000 的计算机，就可以成为“RAS 服务器”，它允许用户使用“拨号网络”登录本机，因此也可以说是一台“拨号网络服务器”，而远程的客户端则称为“拨号网络客户端”。

RAS 服务器扮演着 RAS 客户端与本地网络之间的路由器或网关的角色，让 RAS 客户端能够通过它来连接公司内部网络，访问网络资源，就好像它们是在本地直接连接着网络。一台远程服务器可以同时支持多台远程客户端。远程客户端直接利用调制解调器与本地网络连接，它就如同是在本地的客户端，因此它的操作方式与一般的本地客户端相同。

7.2.2 安装和配置RAS服务器

要让一台安装了 Windows Server 2000 的服务器成为“RAS 服务器”之前，首先要安装好调制解调器（MODEM）。

1．配置RAS服务器MODEM

（1）运行“控制面板”中的“电话和调制解调器选项”应用程序，弹出“调制解调器安装向

导”对话框。单击“添加”按钮后，可以让计算机自动检测 MODEM，也可以选择“不要检测我的调制解调器，我从列表中选择”，这里选择第二种方式，出现“安装新调制解调器”对话框。

（2）在“安装新调制解调器”对话框的“调制解调器”列表中，选择合适的 MODEM 类型，选中后单击“下一步”按钮。如果找不到与你的 MODEM 相匹配的类型，选择“从软盘安装”，同时将你的 MODEM 驱动程序盘插入软驱或光驱，在弹出的“路径输入”对话框中，指定驱动程序所在位置，单击“确定”按钮。

（3）在出现的对话框中选择 MODEM 所连端口，如“通信端口 COM1”，单击“下一步”按钮。系统复制文件，复制结束后，MODEM 的安装完成。

（4）MODEM 安装好后，可以对它进行参数设置和测试，测试 MODEM 安装及工作是否正常。选择“控制面板”中的“电话和调制解调器选项”图标，双击后弹出“电话和调制解调器选项”对话框，选择所安装的 MODEM，按“属性”按钮进入相应的“MODEM 属性”对话框中，在此可以对其参数进行设置，一般不必修改这些参数。

2．配置RAS服务器

为了实现拨号登录远程网络，还要配置远程访问服务器。一般 Windows Server 2000 操作系统安装完成后，“路由和远程访问”组件为默认安装，但相应服务并未启动。配置 RAS 服务器的具体步骤如下：

（1）选择“开始”→“程序”→“管理工具”→“路由和远程访问”，将出现“路由和远程访问”窗口。

（2）右键单击该窗口左边“树”中的“BERRY（本地）”，在弹出的菜单中选择“配置并启用路由和远程访问”项，屏幕出现“路由和远程访问服务安装向导”窗口，单击“下一步”按钮。

（3）在出现的“公共设置”对话框中，选择“远程访问服务器”，单击“下一步”按钮，出现 “远程协议”对话框时，选择现有的协议或者添加新的远程客户协议。如果所需要的通信协议已列在列表中，则单击“下一步”按钮。

（4）出现“IP 地址指定”对话框，可以指定远程客户端获得 IP 地址的方式。若网络中存在 DHCP 服务器，可以由这台 DHCP 服务器为远程客户提供 IP 地址分配；另一种方式是，在本 RAS 服务器上设置一段 IP 地址范围，由 RAS 服务器向远程客户分配 IP 地址。这里选择第二种方式“来自一个指定的地址范围”，按“下一步”按钮，在出现的“地址范围指定”对话框中单击“新建”按钮，设置远程客户端的静态 IP 地址范围（如从 210.43.16.156 到 210.43.16.199），单击“下一步”按钮。

（5）选择不使用 RADIUS，单击“下一步”按钮，最后按“完成”按钮结束配置。配置后的“路由和远程访问”窗口如图 7.4 所示。

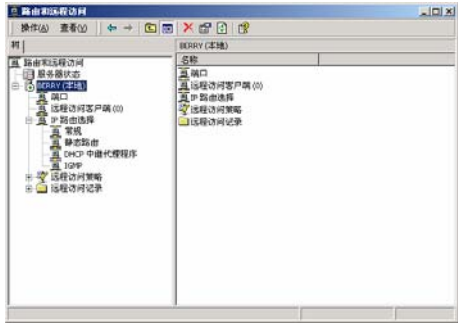


图 7.4　“路由和远程访问”窗口

（6）远程访问服务器具备 DHCP 中继代理程序的功能，以便将拨号网络客户端要求的 IP 地址信息转送给其他网络区域的 DHCP 服务器。如果要设置转送 DHCP 信息，在如图 7.4 所示的窗口中，右键单击“DHCP 中继代理程序”→“属性”，进行相应设定即可。

3．授权用户拨入属性

用户通过拨号登录 RAS 服务器，并能访问网络共享资源，就像使用本地网络一样，如通过网络邻居访问网络中其他计算机上的共享文件夹，这是通过 Internet 访问远程网络所做不到的。

为了能让远程用户拨号登录 RAS 服务器，首先需要对用户进行远程访问授权，使其具有拨号权限。对于网络用户，在域控制器上通过用户管理工具进行授权。选择“服务器管理工具”→“Active Directory 用户和计算机”→“用户”，双击要设置的用户，选择“拨入”选项卡，设置远程访问权限、回拨属性等，如图 7.5 所示。在本例中，将用户 zhang 的远程访问权限设置为“允许访问”和“不回拨”。

如果设置本机用户，则选择菜单“计算机管理”→“系统工具”→“本地用户和组”→“用户”，进行如上设置。

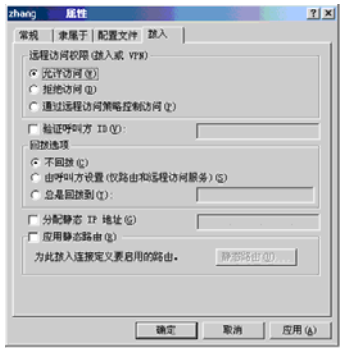


图 7.5　授权用户拨入权限

7.2.3　为接入主机配置拨号连接

RAS 服务器启动工作，客户机如何实现拨号登录 RAS 服务器？这里以客户机运行 Windows 2000 Professional 操作系统为例，介绍客户机配置远程登录服务器的过程。

（1）安装并设置好调制解调器，参见 7.2.2 节的内容。

（2）选择拨号网络，建立新的连接，出现“网络连接向导”，单击“下一步”按钮，在如图 7.6 所示的对话框中选择网络连接类型为“拨号到专用网络”，单击“下一步”按钮。

图 7.6　配置拨号网络

（2）在出现的列表框中选择连接设备，也就是我们刚刚安装的 MODEM，单击“下一步”按钮，出现如图 7.7 所示对话框时，输入远程访问服务器的电话号码，然后单击“下一步” 按钮。此连接设置为只有自己可以使用或让所有用户都可以使用。单击“下一步”按钮，为此连接设置一个名称，单击“完成”按钮结束设置。

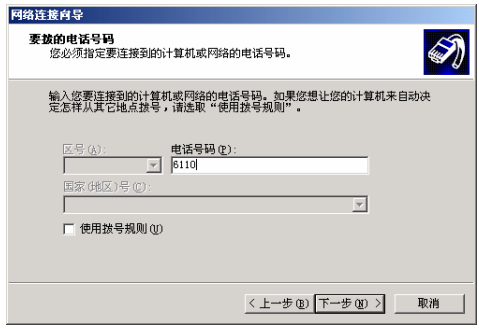


图 7.7　配置 RAS 服务器电话号码

（3）双击新建立的连接，在弹出的对话框中输入用户账号与密码等数据后，单击“拨号”按钮就可以登录到 RAS 服务器。

7.3　构建Intranet

7.3.1　Intranet概述

1．Intranet定义

Intranet 是指采用 Internet 技术（软件、服务和工具），以 TCP/IP 协议作为基础，以 Web 作为核心应用，服务于企业内部事务，将企业内部作业计算机化，以实现企业内部资源共享的网络。简言之，Intranet 是使用企业自有网络来传送信息的私有互联网。

2．Intranet与Internet的关系

（1）Intranet 是一种企业内部的计算机信息网络，而 Internet 是一种向全世界用户开放的公共信息网络，这是两者在功能上的主要区别。

（2）Intranet 是一种利用 Internet 技术、开放的计算机信息网络，它使用 Internet 的各种服务功能（包括 WWW、电子邮件、文件传输与远程登录等），这是 Intranet 与 Internet 两者的共同之处。

（3）Intranet 采用了统一的 WWW 浏览器技术去开发用户端软件，Intranet 用户面对的用户界面与普通 Internet 用户界面相同。因此，企业网内部用户可以很方便地访问 Internet，并使用 Internet 提供的各种服务功能。同时，Internet 用户也能够方便地访问 Intranet。

（4）Intranet 内部信息分为两类：企业内部的保密信息与向社会公众公开的企业产品广告信息。企业内部保密的信息不允许任何外部用户访问，而企业产品广告信息则希望社会上的广大用户尽可能多地访问，防火墙是用来解决 Intranet 与 Internet 互连安全性的重要手段。

7.3.2　Intranet技术要点

1．统一的用户端

用户从标准的统一用户端应该能够访问 Intranet 的所有资源，其应用应该与用户的网络环

境、连网方式、地理位置无关。

2．非结构化信息的发布

各种多媒体信息、各种格式的文本信息均应该有方便、简单的发布方式和更新方式。对于大量文本信息的检索，最好提供全文检索引擎。

3．动态数据库应用

必须提供高效的 Web 与数据库的连接方法，最好有可视化的开发工具。对于企业级的数据库应用，可以采用 API 方式与数据库连接，或者采用标准接口，如 JDBC、ADO 等。

4．消息流机制

应该具备邮件路由和事件触发等工作流功能，使应用系统可以方便地基于 E-mail、Web 等开放标准实现业务流程的网络化。

5．安全技术

Intranet，特别是能访问 Internet 的 Intranet，对安全的考虑是十分重要的。需要确定企业安全需求，并采取相应措施。常用的安全措施有设置防火墙、采用安全服务器代理以及加密技术等。此外，防病毒的措施也是十分重要的。制定清晰的信息网络安全政策和网络用户使用准则，也是安全措施的一个重要问题。

7.3.3 Intranet网络组成

通常，把 Intranet 分成几个子网。不同子网扮演不同角色，实现不同的功能，子网之间用防火墙隔开。子网的划分除了安全因素之外，还与用户数量、服务种类、工作负载等多种因素有关。一般来说，可把 Intranet 划分为接入子网、服务子网和内部子网 3 个子网。图 7.8 是一个典型 Intranet 的网络组成结构示意图。

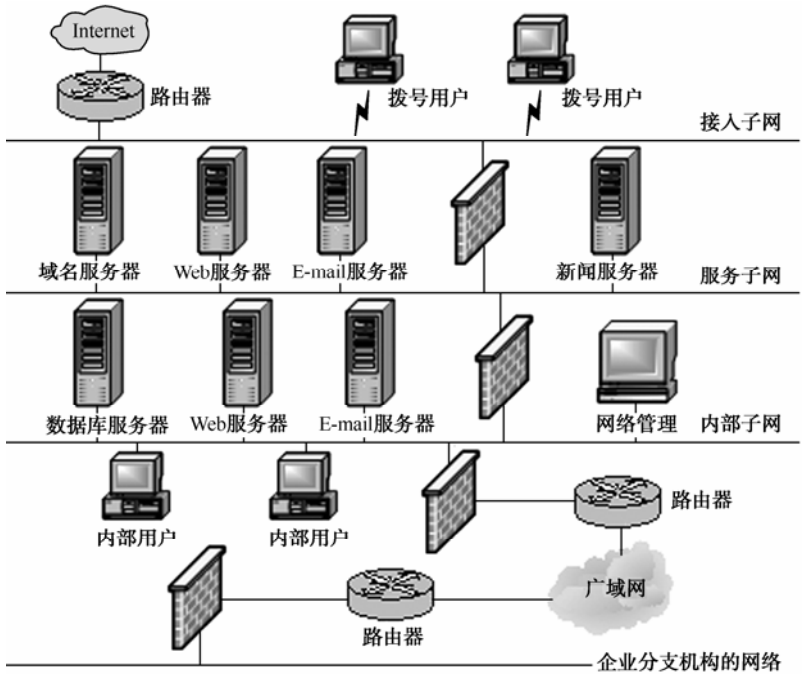


图 7.8　一个典型 Intranet 的网络组成结构示意图

1．接入子网

接入子网也称访问子网。接入子网的作用是提供拨号用户和 Intranet 用户到 Internet 的连接，以及拨号用户到 Internet 之间的路由。

接入子网的核心是路由器，来往于 Internet 的信息都要经过路由器。接入子网与服务子网之间用防火墙隔开，保证所有进入 Intranet 的信息都通过防火墙的过滤。

2．服务子网

服务子网的作用是提供信息服务，主要用于企业向外部发布信息。在服务子网上有 Web 服务器、域名服务器、电子邮件服务器、新闻服务器等，服务子网通过防火墙与内部子网连接。外部用户可以访问服务子网了解企业动态和产品信息。

3．内部子网

内部子网是企业内部使用的网络，是 Intranet 的核心。内部子网包含支持各种服务的企业数据，主要用于企业内部的信息发布与交流、企业内部的管理。因为内部子网上有企业的各种业务数据库，运行着各种应用程序，网络管理也在内部子网上，所以必须采取很强的安全措施。

在内部子网上，除有管理数据库的数据库服务器外，还可以有用于内部信息发布和交流的电子邮件服务器、Web 服务器等。

如果企业在其他地区有分支机构，则需要通过广域网互连，内部子网与广域网之间也要用防火墙隔离。

本 章 小 结

本章主要讲述了以下内容。

（1）用户计算机和用户网络接入 Internet 所采用的技术和接入方式的结构，统称为 Internet 接入技术。Internet 接入网分为主干系统、配线系统和引入线三个部分。Internet 服务提供商（ISP）是为用户提供 Internet 接入和 Internet 信息服务的公司和机构。

（2）Internet 接入技术除了最常见的拨号接入外，还有目前正广泛应用的宽带接入。宽带接入技术主要包括 xDSL 接入技术、HFC 接入技术、以太网接入技术、光纤接入技术等多种有线接入技术以及无线接入技术。

（3）电话拨号接入是个人用户接入 Internet 最早使用的方式之一，接入方法简单、方便，但速度慢，应用单一。

（4）ADSL 接入安装方便，操作简单，无需拨号；利用现有电话线路，上网打电话两不误；提供各种宽带服务，费用适中，速度快，但受距离影响。

（5）HFC 接入利用现有的有线电视网，速度快，是相对比较经济的方式；但信道带宽由整个社区用户共享，用户数增多，带宽就会急剧下降；安全上有缺陷，易被窃听；适用于用户密集型小区。

（6）光纤 FTTx 接入带宽宽，速度快，通信质量高，网络可升级性能好，用户接入简单；提供双向实时业务的优势明显，但投资成本较高，无源光节点损耗大。

（7）ISDN 是普通电话拨号接入和宽带接入之间的过渡方式。DDN 是最常见的专线数据通信线路接入方式。

（8）无线接入是本地有线接入的延伸、补充或临时应急方式。无线接入按接入方式和终

端特征通常分为固定接入和移动接入两大类。

（9）电力线接入利用电力网覆盖面广的优势，但目前技术尚不成熟，仍处于研发中。

（10）通过 RAS，可以实现移动办公；利用电话网接入远程网需要对“拨号网络服务器”和“拨号网络客户端”做相应的配置。

（11）Intranet 是使用企业自有网络来传送信息的私有互联网。

（12）Intranet技术要点：统一的用户端、非结构化信息的发布、动态数据库应用、消息流机制和安全技术。

（13）Intranet 可划分为接入子网、服务子网和内部子网 3 个子网。

思 考 题

1．什么是 Internet 接入技术？常用的接入技术有哪些？

2．何谓宽带网络？常用的宽带接入技术有哪几种？

3．什么是 ADSL？简述基于 ADSL 的接入网的构成。

4．简述 HFC 技术的组成、特点和应用。

5．光纤接入网的接入方式有哪些？

6．无线接入网有哪几种形式？

7．什么是 Intranet，它与 Internet 有什么关系？

8．简述 Intranet 的组成。

第 8 章　计算机网络安全

本章要点

目前，在服务器的操作系统平台上，受广大用户欢迎的有 UNIX、Linux 和 Windows NT。这三个操作系统存在不少安全漏洞。如果不了解这些漏洞，不采取相应的对策和防范措施，就会使系统完全暴露在入侵者的入侵范围之内，随时有可能遭受毁灭性攻击。

本章将从上述问题着手，讨论系统特性、安全策略及常见的网络安全配置。

本章目标

- 了解网络安全的概念和网络安全面临的威胁
- 了解病毒的定义及病毒防治方法
- 掌握防火墙的概念、防火墙的分类和主要技术
- 了解密码学的基本概念
- 了解身份认证技术、消息认证技术和数字签名

8.1　网络安全概述

随着计算机网络技术的发展和应用，丰富的网络信息资源给用户带来了极大的方便，但同时，网络病毒、黑客入侵、恶性代码、垃圾邮件等网络安全问题表现得更为突出。据统计，全球约每 20s 就发生一次计算机入侵事件，Internet 上的网络防火墙约 1/4 被突破，约 70%以上的网络主管人员报告因机密信息泄露而受到损失。

8.1.1　网络安全的概念

网络安全是一个相对的概念，其本质是网络信息的安全问题。从广义上讲，凡是涉及网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。狭义的网络安全指网络系统的硬件、软件及其系统中的数据受到保护，避免因偶然的或者恶意的原因而遭到破坏、更改、泄露，保证系统能连续、可靠地运行，网络服务不中断。

一个安全的计算机网络应当包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等。

网络安全的目标主要表现在以下方面：

（1）可靠性。可靠性是网络安全的最基本要求之一。可靠性主要包括硬件可靠性、软件可靠性、人员可靠性、环境可靠性。

（2）可用性。可用性是网络系统面向用户的安全性能，要求网络信息可被授权实体访问并按要求使用，包括对静态信息的可操作性和动态信息的可见性。

（3）保密性。保密性建立在可靠性和可用性基础上，保证网络信息只能由授权的用户读

取。常用的信息保密技术有防侦听、信息加密和物理保密。

（4）完整性。完整性要求网络信息未经授权不能进行修改，网络信息在存储或传输过程中要保持不被偶然或蓄意地删除、修改、伪造等，防止网络信息被破坏和丢失。

8.1.2 计算机网络面临的安全威胁

计算机网络面临的安全威胁如图 8.1 所示，主要有截获、中断、篡改和伪造 4 种。

（1）截获——从网络上窃听他人的通信内容。

（2）中断——有意中断他人在网络上的通信。

（3）篡改——故意篡改网络上传送的报文。

（4）伪造——伪造信息在网络上传送。

上述四种威胁可划分为两大类，即主动攻击和被动攻击。截获信息的攻击称为被动攻击，而更改信息和拒绝用户使用资源的攻击称为主动攻击。在被动攻击中，攻击者只是观察和分析某一个协议数据单元 PDU（Protocol Data Unit，协议数据单元）而不干扰信息流。主动攻击是指攻击者对某个连接中通过的 PDU 进行各种处理。

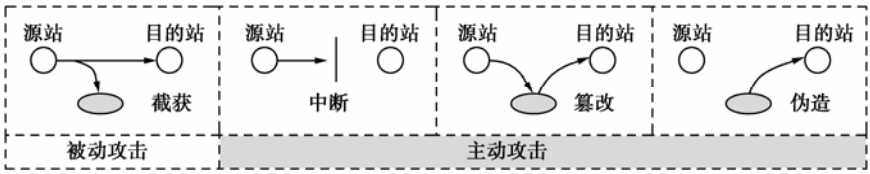


图 8.1　网络面临的安全威胁

对于主动攻击，可以采取适当措施加以检测。但是，对于被动攻击，通常是检测不出来的。对付被动攻击可以采用各种数据加密技术，而对付主动攻击，则需将加密技术与适当的鉴别技术相结合。

还有一种特殊的主动攻击，即恶意程序的攻击。恶意程序种类繁多，对网络安全威胁较大的主要有以下 4 种。

（1）计算机病毒：一种会“传染”其他程序的程序，“传染”是通过修改其他程序来把自身或其变种复制进去完成的。

（2）计算机蠕虫：通过网络的通信功能将自身从一个节点发送到另一个节点并启动运行的程序。

（3）特洛伊木马：一种程序，它执行的功能超出所声称的功能。

（4）逻辑炸弹：一种当运行环境满足某种特定条件时执行其他特殊功能的程序。

8.1.3 计算机网络安全的内容

从技术的角度看，计算机网络安全的内容涉及网络实体安全、网络软件安全、网络数据安全和网络安全管理等方面。

（1）网络实体安全：包括计算机系统机房环境和设施的安全保护，计算机硬件、网络设备及传输线路的安全。

（2）网络软件安全：保护网络系统不被入侵，系统软件和应用软件不被非法复制、篡改以及受到病毒的侵害。

（3）网络数据安全：保护网络信息数据不被非法存取，保护数据的完整性和一致性。

（4）网络安全管理：采取计算机安全技术，建立安全管理制度，开展安全审计等。

8.2 病毒

8.2.1 病毒概述

1．病毒定义

按《中华人民共和国计算机信息系统安全保护条例》中的规定，计算机病毒指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据、影响计算机使用并能自我复制的一组计算机指令或者程序代码。

一般的病毒包括特洛伊木马、病毒、细菌和蠕虫等。特洛伊木马和病毒不能脱离某些特定的应用程序、应用工具或系统而独立存在；而细菌和蠕虫是完整的程序，操作系统可以调度和运行它们。除特洛伊木马外，其他三种形式的病毒都能够复制。

2．病毒分类

病毒从不同的角度有不同的分类。按危害性分为良性病毒和恶性病毒；按寄生方式分为代替式病毒、链接式病毒、转储式病毒、填充式病毒和覆盖式病毒等。按病毒感染的途径，病毒分为下列 3 类。

（1）引导型病毒。引导型病毒是藏匿在磁盘片或硬盘的第一个扇区里。每次启动计算机时，在操作系统还没被加载之前就被加载到内存中，这个特性使得病毒完全控制 DOS 的各类中断，并且拥有更大的能力进行传染与破坏。这类病毒也称磁盘引导区病毒，如“Michelangelo”、“Disk Killer”等病毒。

（2）文件型病毒。文件型病毒通常寄生在可执行文件中，如*.COM、*.EXE 等。当这些文件被执行时，病毒的程序就跟着被执行。这类病毒也称为可执行文件病毒、应用程序病毒或操作系统病毒。

（3）复合型病毒。这类病毒兼具有引导型病毒以及文件型病毒的特性。它们可以传染*.COM 和*.EXE 文件，也可以传染磁盘的引导区。由于这个特性，使得这种病毒具有相当程度的传染力，一旦发病，其破坏性相当大，如“Flip”等病毒。

3．病毒的网络威胁

目前，病毒对网络的威胁主要表现在：

（1）工作站受到的威胁。病毒对网络工作站的攻击途径主要包括利用软盘读/写进行传播、通过网络共享进行攻击、通过电子邮件系统进行攻击、通过 FTP 下载进行攻击和通过 WWW 浏览进行攻击。

（2）服务器受到的威胁。网络操作系统一般都采用 Windows NT/2000 Server 和少量 UNIX/Linux，而 UNIX/Linux 本身的计算机病毒的流行报告几乎很少。早期 Windows NT 系统对病毒有一定免疫能力，但到目前为止，感染 Windows NT 系统的病毒已有一定数量。

（3）Web 站点受到的威胁。一般 Web 站点的用户访问量很大，目前能通过 Web 站点传播的病毒只有脚本蠕虫、一些恶意 Java 代码和 ActiveX。

8.2.2 蠕虫和特洛伊木马

蠕虫和特洛伊木马程序是病毒程序。

1．蠕虫

传统意义上的计算机蠕虫程序，通过网络连接从一个系统向另一个系统传播。与病毒类似，蠕虫也在计算机与计算机之间自我复制，但蠕虫病毒可自动完成复制过程，蠕虫病毒复制自身时会使用一些网络工具，如电子邮件、远程执行功能和远程登录功能。一旦计算机感染了蠕虫病毒，蠕虫即可自传播。最危险的是，蠕虫可大量复制。例如，蠕虫可向电子邮件地址簿中的所有联系人发送自己的副本，联系人的计算机也将执行同样的操作，结果造成多米诺骨牌效应（网络通信负担沉重），业务网络和整个 Internet 的运行速度都将减慢。

网络蠕虫有休眠期、传播期、触发期和执行期。蠕虫程序首先检查主机或其他存放远程系统地址的类似文件，搜索可供感染的其他系统；然后与远程系统建立连接，把自身复制到远程系统中，同时运行该副本。蠕虫在向系统复制自身之前会试图确定系统以前是否感染过。

典型的网络蠕虫有“冲击波”（阻塞网络）、“小邮差”（发带毒邮件）等。

2．特洛伊木马

“特洛伊木马”原指古希腊兵藏在木马内进入敌方城市，从而占领敌方城市的故事。正像历史上的“木马”一样，称为“木马”的程序也是一种掩藏在美丽外表下潜入计算机内部的计算机病毒。

特洛伊木马程序就是隐藏了意外内容的应用程序，这些意外内容可以是一个过程或函数，由特洛伊木马程序编写者专门加到程序中，完成用户不了解、可能也不许可的活动。当未授权用户无法直接完成某些操作时，就可以通过特洛伊木马程序来间接完成。另外一种很难被检测到的特洛伊木马程序是编译器，通过修改正常的编译器，就可以在编译某些程序时插入附加代码，附加代码会在程序中留下后门，而通过阅读原来程序的源代码是发现不了这些特洛伊木马程序的。

特洛伊木马程序与病毒程序不同，它不进行复制，也不把自身加入到其他文件中。特洛伊木马程序是一个独立的程序，其源代码包含破坏性内容。

常见的木马程序有“网银大盗”、“灰鸽子”、“QQ 大盗”等。

8.2.3 病毒防治

对付病毒的最理想方法是预防，加强预防措施可以减少病毒攻击的成功次数。下列技术和措施可用于防止病毒感染：

（1）对新系统做彻底的扫描，在安装防病毒软件之前，必须确保系统没有感染病毒。

（2）建立访问控制策略，对每个用户设置正确的权限级别，防止恶意程序的传播。

（3）监视进程，观察不同的系统活动，拦截所有可疑行为。

（4）安装防病毒软件并及时更新病毒库，每周应至少更新一次病毒库。

（5）不从不可靠的渠道下载任何软件。

（6）使用基于客户端的防火墙或过滤措施。

一旦检测到病毒就需确定病毒的位置，以便识别出已感染程序中的病毒类型，然后去除已感染程序中的所有病毒痕迹，恢复到最初的状态。如果检测到病毒但无法识别也无法去除，则需丢弃已感染的程序，重新安装该程序的备份文件。

常用的防病毒软件有金山毒霸、瑞星、江民、卡巴斯基、Norton、MACfee 等。

8.3 防火墙

8.3.1 防火墙的概念

防火墙（Firewall）是一道介于公共网与内部网之间的屏障，由一个或一组系统组成，可用来解决内部网和外部网的安全问题。防火墙在互连的网络中的位置如图 8.2 所示。防火墙是由软件、硬件构成的系统，是一种特殊编程的路由器，用来在两个网络之间实施接入控制策略。接入控制策略是由使用防火墙的单位自行制定的，目的是适合本单位的需要。

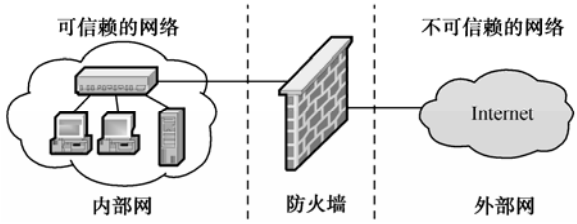


图 8.2 防火墙在互连的网络中的位置

防火墙的功能有两个：一是阻止，二是允许。“阻止”就是阻止某种类型的通信量通过防火墙（从外部网到内部网或从内部网到外部网）。“允许”的功能与“阻止”恰好相反。可见，防火墙必须能够识别通信量的各种类型。防火墙的主要功能是“阻止”。

8.3.2 防火墙的主要技术

防火墙的主要 3 种技术是包过滤、网络地址翻译和应用级代理。

1．包过滤

包过滤（Packet Filtering）是在网络层依据系统的过滤规则，对数据包进行选择和过滤，这种规则又称为访问控制表（ACL）。该技术通过检查数据流中的每个数据包的源地址、目标地址、源端口、目的端口及协议状态或它们的组合来确定是否允许该数据包通过。这种防火墙通常安装在路由器上。

一般而言，包过滤包括两种基本类型：无状态检查的包过滤和有状态检查的包过滤，其区别在于后者通过记住防火墙的所有通信状态，并根据状态信息来过滤整个通信流，而不仅仅是包。另外，两者均被配置为只过滤最有用的数据域，包括协议类型、IP 地址、TCP/UDP 端口、分段口和源路由信息，但还是有许多方法可绕过包过滤器进入 Internet，这是因为：

（1）TCP 只能在第 0 个分段中被过滤。

（2）特洛伊木马可以使用 NAT 使包过滤器失效。

（3）许多包过滤器允许 1024 以上的端口通过。

因此，“纯”包过滤器的防火墙不能完全保证内部网的安全，必须与代理服务器和网络地址翻译结合起来才能解决问题。

2．网络地址翻译

网络地址翻译（Network Address Translation，NAT）的最初设计目的是增加在专用网络

中可使用的 IP 地址数，但现在则用于屏蔽内部主机。NAT 通过将专用网络中的专用 IP 地址转换成在 Internet 上使用的全球惟一的公共 IP 地址，实现对黑客有效地隐藏所有 TCP/IP 级的有关内部主机信息的功能，使外部主机无法探测到它们。

NAT 实质上是一个基本的代理：一个主机充当代理，代表内部所有主机发出请求，从而将内部主机的身份从公用网上隐藏起来。许多防火墙都支持不同类型的网络地址翻译。

由于 NAT 仅在传输层上实现，所以隐藏在 TCP/IP 通信中有效的数据信息可以传输到高层，并且可用来寻找在高层通信中的缺点或者用来与特洛伊木马通信。

3．应用级代理

开发应用级代理的最初目的是对 Web 进行缓存，减少冗余访问，但现在主要用于防火墙。代理服务器通过侦听网络内部客户的服务请求，检查并验证其合法性。若合法，它将作为一台客户机一样向真正的服务器发出请求并取回所需信息，最后再转发给客户机。对于内部客户机而言，代理服务器好像原始的公共服务器；对于公共服务器而言，代理服务器好像原始的客户机一样，即代理服务器充当了双重身份，并将内部系统与外界完全隔离开来，外面只能看到代理服务器，而看不到任何内部资源。

虽然代理服务被认为是最安全的防火墙技术，但由于代理软件不能保护操作系统不受服务拒绝攻击，也不能保护对在服务器上运行的其他服务的攻击，所以纯代理仍有许多安全问题，并且效率低下。因此，大多数实际的安全代理的实现产品都包括包过滤功能和网络翻译来形成一个完整的防火墙。

8.3.3　常见的防火墙设计方案

最简单的防火墙配置，就是直接在内部网和外部网之间加装一个包过滤路由器或者应用网关。为更好地实现网络安全，有时还要将几种防火墙技术组合起来构建防火墙系统。目前，比较流行的有以下三种防火墙配置方案。

1．双宿主机网关（Dual Homed Gateway）

这种配置是用一台装有两个网络适配器的双宿主机做防火墙，如图 8.3 所示。双宿主机用两个网络适配器分别连接两个网络，通常称为堡垒主机。堡垒主机上运行着防火墙软件（代理服务器），可以转发应用程序的数据，提供服务等。双宿主机网关有一个致命弱点：一旦入侵者侵入堡垒主机并使该主机只具有路由器功能，则任何网上用户均可以随便访问有保护的内部网。

图 8.3　双宿主机网关

2．屏蔽主机网关（Screened Host Gateway）

屏蔽主机网关易于实现，安全性好，应用广泛。屏蔽主机分为单宿堡垒主机和双宿堡垒主机。

单宿堡垒主机由一个包过滤路由器连接外部网，同时一个堡垒主机安装在内部网上，如

图 8.4 所示。堡垒主机只有一个网卡，与内部网连接。通常，在路由器上设立过滤规则，并使这个单宿堡垒主机成为从 Internet 惟一可以访问的主机，确保了内部网不受未被授权的外部用户的攻击。Intranet 内部的客户机，可以受控制地通过屏蔽主机和路由器访问 Internet。

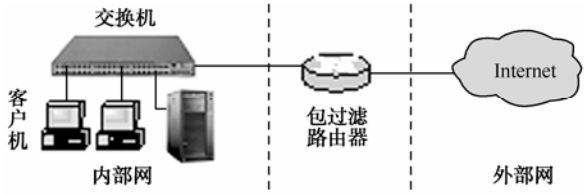


图 8.4　单宿堡垒主机

双宿堡垒主机与单宿堡垒主机的区别是，双宿堡垒主机有两块网卡：一块连接内部网，另一块连接包过滤路由器，如图 8.5 所示。双宿堡垒主机在应用层提供代理服务，比单宿堡垒主机更加安全。

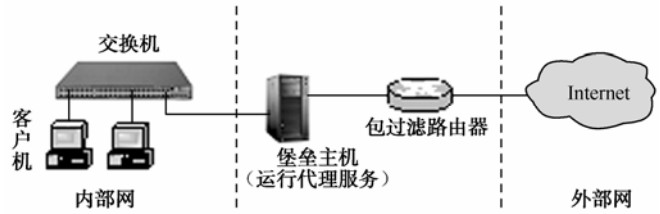


图 8.5　双宿堡垒主机

3．屏蔽子网（Screened Subnet）

这种方法是在 Intranet 与 Internet 之间建立一个被隔离的子网，用两个包过滤路由器将这一子网分别与 Intranet、Internet 分开，如图 8.6 所示。两个包过滤路由器放在子网的两端，在子网内构成一个“缓冲地带”，两个路由器中的一个控制 Intranet 数据流，另一个控制 Internet 数据流，Intranet 和 Internet 均可访问屏蔽子网，但禁止它们穿过屏蔽子网通信。可根据需要在屏蔽子网中安装堡垒主机，为内部网和外部网的互相访问提供代理服务，但是来自两个网的访问都必须通过两个包过滤路由器的检查。对于向 Internet 公开的服务器，如 WWW、FTP、Mail 等 Internet 服务器也可安装在屏蔽子网内，这样无论是外部用户，还是内部用户都可访问。这种结构的防火墙安全性能高，具有很强的抗攻击能力，但需要的设备多、造价高。

图 8.6　屏蔽子网

当然，防火墙本身也有其局限性，如不能防范绕过防火墙的入侵，像一般的防火墙不能防止受到病毒感染的软件或文件的传输；难以避免来自内部的攻击等。总之，防火墙只是一种整体安全防范策略的一部分，仅有防火墙是不够的，安全策略还必须包括全面的安全准则，

即网络访问、本地和远程用户认证、拨出拨入呼叫、磁盘和数据加密以及病毒防护等有关的安全策略。

8.3.4 分布式防火墙技术方案

传统的防火墙设置在网络边界，处于内、外部互联网之间，称为“边界防火墙（Perimeter Firewall）”。随着人们对网络安全防护要求的提高，边界防火墙明显感觉到力不从心，因为给网络带来安全威胁的不仅是外部网，更多的是来自内部网。边界防火墙无法对内部网实现有效的保护，除非每一台主机都安装防火墙，但这是不可能的。因此，一种新型的防火墙技术，即分布式防火墙（Distributed Firewall）技术产生了。

分布式防火墙可以很好地解决边界防火墙的不足。当然，不是为每台主机安装防火墙，而是把防火墙的安全防护系统延伸到网络中每台主机。一方面，有效地保证了用户的投资不会很高；另一方面，给网络带来的安全防护是非常全面的。

在新的安全体系结构下，分布式防火墙代表新一代防火墙技术的潮流，它可以在网络的任何交界和节点处设置屏障，从而形成了一个多层次、多协议，内外皆防的全方位安全体系。它的主要优势如下。

（1）增强的系统安全性：增加了针对主机的入侵检测和防护功能，加强了对来自内部攻击的防范，可以实施全方位的安全策略。

（2）提高了系统性能：消除了结构性瓶颈问题，提高了系统性能。

（3）系统的扩展性：分布式防火墙随系统扩充提供了安全防护无限扩充的能力。

（4）实施主机策略：对网络中的各节点可以起到更安全的防护。

（5）应用更为广泛，支持 VPN 通信。

因为分布式防火墙采用了软件形式（有的采用了软件＋硬件形式），所以功能配置更加灵活，具备充分的智能管理能力，总的来说可以体现在以下 6 个方面。

（1）Internet 访问控制：依据工作站名称、设备指纹等属性，使用“Internet 访问规则”，控制该工作站或工作站组在指定的时间段内是否允许/禁止访问模板或网址列表中所规定的 Internet Web 服务器，某个用户可否基于某工作站访问 WWW 服务器，同时当某个工作站/用户达到规定流量后是否断网。

（2）应用访问控制：通过对网络通信从链路层、网络层、传输层、应用层基于源地址、目标地址、端口、协议的逐层包过滤与入侵监测，控制来自局域网/Internet 的应用服务请求，如 SQL 数据库访问、IPX 协议访问等。

（3）网络状态监控：实时动态报告当前网络中所有的用户登录、Internet 访问、内部网访问、网络入侵事件等信息。

（4）黑客攻击的防御：抵御包括 Smurf 拒绝服务攻击、ARP 欺骗式攻击、Ping 攻击、Trojan 木马攻击等的近百种来自网络内部以及来自 Internet 的黑客攻击手段。

（5）日志管理：管理对工作站协议规则日志、用户登录事件日志、用户 Internet 访问日志、指纹验证规则日志、入侵检测规则日志的记录与查询分析。

（6）系统工具：包括系统层参数的设定、规则等配置信息的备份与恢复、流量统计、模板设置、工作站管理等。

8.3.5 防火墙的选购

目前，企业主要采用防火墙来防止内部网可能所受到的攻击（包括黑客入侵、内部信息泄露、不良信息进入内部网等）。市面上的网络防火墙设备不仅品牌繁多，而且各种不同档次的产品也让人眼花缭乱，使普通用户无所适从。如何选择能够适应自己企业的需要、达到最大安全效果的防火墙产品呢？选择防火墙的主要标准如下。

（1）总拥有成本。防火墙产品作为网络系统的安全屏障，其总拥有成本不应该超过受保护网络系统可能遭受最大损失的成本。

（2）防火墙本身的安全。作为信息系统安全产品，防火墙本身应该是安全的，不给外部入侵者可乘之机。

（3）管理与培训。管理和培训是评价一个防火墙好坏的重要方面。人员的培训和日常维护费用通常会在总拥有成本中占据较大的比例。

（4）可扩充性。好产品应该留给用户足够的弹性空间，在安全水平要求不高的情况下，只选购基本系统，而随着要求的提高，用户仍然有进一步增加选件的余地，这样能够保护用户的投资。

（5）防火墙的安全性能。防火墙产品最难评估的是防火墙的安全性能，即防火墙是否能够有效地阻挡外部入侵。

8.4 加密技术

8.4.1 密码学的基本概念

许多计算机系统采用口令机制来控制对系统资源的访问，当用户想要访问受保护的资源时，就会被要求输入口令。在传统的计算机系统中，简单的口令机制就能取得很好的效果，因为系统本身不会把口令泄露出去；而在网络系统中，这样的口令就很容易被窃听。比如，某用户从网络登录到一台远程计算机上，如果数据是以明码的形式传输的，就很容易在网络传输线路上被窃取，这种技术称为在线窃听。在线窃听在局域网上更容易实现，因为大多数局域网都是总线结构，从理论上讲，任一台计算机都可以截取网上的所有数据帧。为了保证数据的保密性，必须对数据进行加密。

密码技术是对存储或者传输的信息采取秘密交换以防止第三者对信息窃取的技术。密码技术涉及以下术语。

（1）明文：待加密的报文或数据。

（2）密文：加密后的报文或数据。

（3）密钥：用于加密和解密的钥匙，通常是一个字符串。

（4）加密算法：加密所采用的变换方法。

（5）加密：把明文转换成密文的过程。

（6）解密：对密文实施与加密相逆的变换，从而获得一个字符串。

密码技术分为加密和解密两部分。加密是把需要加密的报文（简称明文）按照密钥参数进行变换，产生密码文件（简称密文）。解密是按照密钥把密文还原成明文的过程。密钥是一个数值，它和加密算法一起生成特别的密文。密钥是非常大的数，密钥规模用位（bit）表示，在公开密钥加密方法中，密钥规模越大，密文就越安全。利用密码技术，在信源和通信信道

之间对报文进行加密，经过信道传输，到信宿接收时进行解密，以实现网络通信保密。一般的数据加密与解密模型如图 8.7 所示。

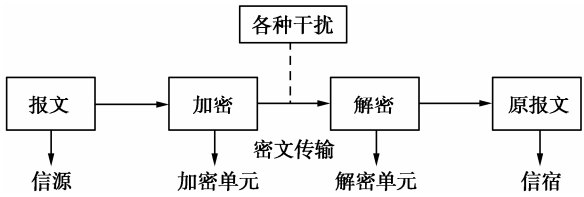


图 8.7　一般的数据加密与解密模型

密码编码学是密码体制的设计学，而密码分析学则是在未知密钥的情况下从密文推演出明文或密钥的技术。密码编码学与密码分析学组合形成密码学。

如果不论截取者获得了多少密文，但在密文中都没有足够的信息来惟一地确定出对应的明文，则这一密码体制称为无条件安全的，或称为理论上是不可破译的。在无任何限制的条件下，目前几乎所有实用的密码体制都是可破译的。因此，人们关心的是要研制出在计算机上（而不是在理论上）是不可破译的密码体制。如果一个密码体制中的密码不能被可以使用的计算资源破译，则这一密码供给制称为在计算上是安全的。

根据加密方和解密方使用的密钥是否相同，可将密码技术分成对称密钥体制和非对称密钥体制。

8.4.2　对称密钥体制

对称密钥体制是从传统的简单换位、代替密码发展而来的，也称为私钥密码体制。对称密钥体制使用相同的密钥加密和解密信息，即通信双方建立并共享一个密钥。

1．对称密钥体制的工作原理

对称密钥体制的工作原理如图 8.8 所示。用户 A 要传送机密信息给用户 B，则用户 A 和用户 B 必须共享一个预先由人工分配或由一个密钥分发中心（KDC）分发的密钥 K，于是用户 A 用密钥 K 和加密算法 E 对明文 P 加密得到密文 C，并将密文 C 发送给用户 B；用户 B 用同样的密钥 K 和解密算法 D 对密文解密，得到明文 P。

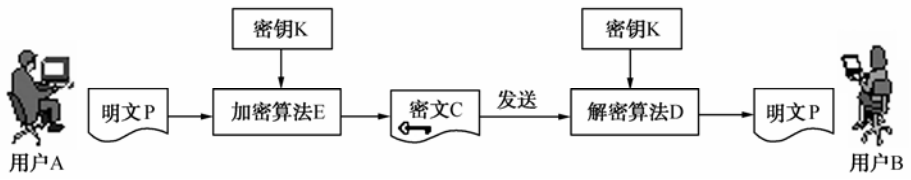


图 8.8　对称密钥体制的工作原理

2．DES 和 AES

DES（Data Encryption Standard，数据加密标准）是使用最为广泛的一种加密方案，一般认为是很难破解的私钥。它以 64 位的块来加密，即通过对 64 位的明文块加密得到 64 位的密文块。加密和解密都使用相同的密钥和算法，只是在密钥次序中有些区别。56 位的密钥表示为 64 位的数，而每个第 8 位都用于奇偶校验。DES 可用于 ECB、CBC、CFB 和 OFB 等模式。但是，一般 DES 只用于 CBC 模式和 CFB 模式。

但是在 1997 年，全国范围的计算机网络用户首次用了 140 天攻破了 DES 密钥，而且随着处理速度的增加，破解 DES 密钥的时间变得越来越短。因此，美国政府提出了一个项目，由“美国国家标准技术研究所（NIST）”负责，目的是找出一种加密算法，作为政府的新标准替换 DES，此算法称为“高级加密算法（Advanced Encryption Standard，AES）”。

从 NIST 发布的文档可以看出，AES 应满足如下条件：

（1）算法必须是对称密码或私有密码。

（2）算法必须是类似 DES 的块密码，而不是流密码。

（3）算法支持密钥长度范围为 128～256 位，而且算法还应支持不同块数的数据。

（4）算法应该用 C 或 Java 程序语言设计。

除上述需求外，AES 还必须具有高效率，而且 AES 算法必须公开，免专利权税。

8.4.3 非对称密钥体制

非对称密钥体制也称为公开密钥体制，是现代密码学中最重要的发明和进展。非对称密钥体制不同于传统的对称密钥体制，它要求密钥成对出现，一个为公共密钥，另一个为专用密钥，并且不可能从其中一个推导出另一个。公共密钥作为加密密钥，以用户专用密钥作为解密密钥，实现多个用户加密的消息只能由一个用户解读。以用户专用密钥作为加密密钥、以公开密钥作为解密密钥，可实现由一个用户加密的消息供多个用户解读。前者用于保密通信，后者用于数字签名。公共密钥发布出去，专用密钥要保证绝对的安全。用公共密钥加密的信息只能用专用密钥解密，反之亦然。由于非对称密钥体制不需要联机密钥服务器，密钥分配协议简单，所以极大简化了密钥管理。除加密功能外，非对称密钥体制还可以提供数字签名。非对称密钥体制的加密算法主要有 RSA、Fertezza、EIGama 等。

1．非对称密钥体制的原理

非对称密钥体制的原理为：用户 A 和用户 B 各自拥有一对密钥（KA、KA-1）和（KB、KB-1）。私钥 KA-1、KB-1 分别由用户 A、用户 B 各自秘密保管，而公钥 KA、KB 则以证书的形式对外公布。当用户 A 要将明文 P 安全地发送给用户 B 时，则用户 A 用用户 B 的公钥 KB 加密 P 得到密文 C；而用户 B 收到密文 P 后，用私钥 KB-1 解密恢复明文 P。

非对称密钥体制的优点是，尽管通信双方不认识，但只要提供密钥的 CA 可靠，就可以进行安全通信，这正是 Web 商务所要求的。

非对称密钥与私钥密码相比，处理速度慢，因此，通常把非对称密钥与对称密钥结合起来，即用非对称密钥在通信双方之间传送对称密钥中的密钥，而用对称密钥来对实际传输的数据加密、解密。另外，对称密钥也用来对非对称密钥进行加密。

2．RSA 密码系统

非对称密钥加密的第一个算法是由 Ralph Merkle 和 Martin Hellman 开发的背包算法，它只能用于加密。后来，Adi Shamir 将其改进，使之能用于数字签名。背包算法的安全性不好，也不完善。不久后，出现了第一个较完善的公开密钥算法 RSA。RSA 密码系统的安全性基于大素数分解的困难性，其理论基础是数论的欧拉定理，即寻求两个大素数容易，但将它们的乘积进行因式分解极其困难。

非对称密钥算法中使用得最广的是 RSA。RSA 使用两个密钥：一个是公共密钥；另一个是专用密钥。如果用其中一个加密，则用另一个解密，密钥长度为 40～2048 位可变，加密时也把明文分成块，块的大小可变，但不能超过密钥的长度，RSA 算法把每一块明文转化为与

密钥长度相同的密文块。因为密钥越长，加密效果越好，但加密、解密的开销也大，所以要在安全与性能之间折中考虑，一般 64 位是较合适的。RSA 的一个比较知名的应用是 SSL。在美国和加拿大，SSL 采用 128 位 RSA 算法。由于出口限制，在其他地区（包括中国）通用的是 40 位版本。

8.4.4 数字信封技术

数字信封是公钥密码体制在实际中的一个应用，是用加密技术来保证只有规定的特定收信人才能阅读通信的内容。

在数字信封中，信息发送方采用对称密钥来加密信息内容，然后将此对称密钥用接收方的公开密钥来加密（这部分称为数字信封）之后，将它和加密后的信息一起发送给接收方；接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开加密信息。这种技术的安全性相当高。数字信封主要包括数字信封打包和数字信封拆解（如图 8.9 所示），数字信封打包是使用对方的公钥将加密密钥进行加密的过程，只有对方的私钥才能将加密后的数据（通信密钥）还原；数字信封拆解是使用私钥将加密过的数据解密的过程。

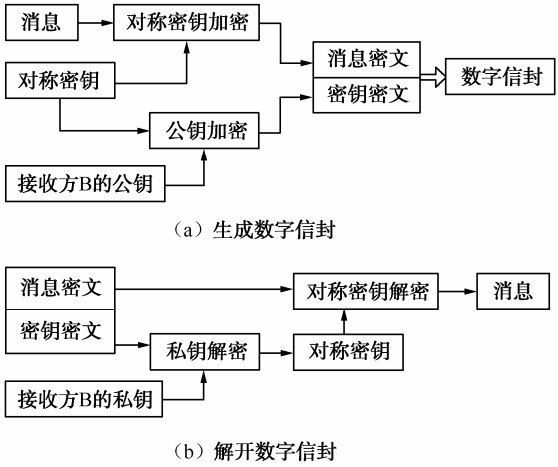


图 8.9　数字信封打包和数字信封拆解

数字信封的功能类似于普通信封，普通信封在法律的约束下保证只有收信人才能阅读信的内容；数字信封采用密码技术保证只有规定的接收人才能阅读信息的内容。数字信封中采用了对称密码体制和公钥密码体制。信息发送者首先利用随机产生的对称密码加密信息，再利用接收方的公钥加密对称密码，被公钥加密后的对称密码称为数字信封。在传递信息时，信息接收方若要解密信息，必须先用自己的私钥解密数字信封，得到对称密码，才能利用对称密码解密所得到的信息。这样就保证了数据传输的真实性和完整性。

在一些重要的电子商务交易中，密钥必须经常更换。为了解决每次更换密钥的问题，结合对称加密技术和公开密钥技术的优点，它克服了秘密密钥加密中秘密密钥分发困难和公开密钥加密中加密时间长的问题，使用两个层次的加密来获得公开密钥技术的灵活性和秘密密钥技术的高效性。信息发送方使用密码对信息进行加密，从而保证只有规定的收信人才能阅读信的内容。采用数字信封技术后，即使加密文件被他人非法截获，但因为截获者无法得到发送方的通信密钥，故不可能对文件进行解密。

8.5 网络安全认证技术

8.5.1 网络安全认证技术的概况

网络安全认证技术是网络安全技术的重要组成部分之一。认证指的是证实被认证对象是否属实和是否有效的一个过程，其基本思想是通过验证被认证对象的属性来达到确认被认证对象是否真实有效的目的。被认证对象的属性可以是口令、数字签名或指纹、声音、视网膜这样的生理特征。

认证常常用于通信双方相互确认身份，以保证通信的安全。认证一般可以分为下列两种。

（1）身份认证：用于鉴别用户身份。

（2）消息认证：用于保证信息的完整性和抗否认性；在很多情况下，用户要确认网上信息的真假，信息是否被第三方修改或伪造，这就需要消息认证。

8.5.2 身份认证技术

认证（Authentication）是证实实体身份的过程，是保证系统安全的重要措施之一。当服务器提供服务时，需要确认来访者的身份，访问者有时也需要确认服务提供者的身份。

身份认证是指计算机及网络系统确认操作者身份的过程。计算机网络系统是一个虚拟的数字世界。在这个数字世界中，一切信息（包括用户的身份信息）都是用一组特定的数据来表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。现实世界是一个真实的物理世界，每个人都拥有独一无二的物理身份。如何保证以数字身份进行操作的操作者就是这个数字身份的合法拥有者，也就是说，保证操作者的物理身份与数字身份相对应，就成为一个很重要的问题。身份认证技术的诞生就是为了解决这个问题。

如何通过技术手段保证用户的物理身份与数字身份相对应呢？在真实世界中，验证一个人的身份主要通过以下三种方式判定。

（1）根据你所知道的信息来证明你的身份（what you know），假设某些信息只有某个人知道，如暗号等，通过询问这个信息就可以确认这个人的身份。

（2）根据你所拥有的东西来证明你的身份（what you have），假设某一个东西只有某个人有，如印章等，通过出示这个东西也可以确认个人的身份。

（3）直接根据你独一无二的身体特征来证明你的身份（who you are），如指纹、面貌等。

在信息系统中，一般来说，下列三个要素可以用于认证过程。

（1）用户的知识（Knowledge），如口令等。

（2）用户的物品（Possession），如 IC 卡等。

（3）用户的特征（Characteristic），如指纹等。

现在，计算机及网络系统中常用的身份认证方法如下：

（1）身份认证技术从是否使用硬件来看，可以分为软件认证和硬件认证。

（2）从认证需要验证的条件来看，可以分为单因子认证和双因子认证。

（3）从认证信息来看，可以分为静态认证和动态认证。

身份认证技术的发展，经历了从软件认证到硬件认证，从单因子认证到双因子认证，从静态认证到动态认证的过程。下面介绍常用的身份认证方法。

1．基于口令的认证方法

传统的认证技术主要采用基于口令的认证方法。当被认证对象要求访问提供服务的系统时，提供服务的认证方要求被认证对象提交该对象的口令，认证方收到口令后，将其与系统中存储的用户口令进行比较，以确认被认证对象是否为合法访问者。这种认证方法的优点：一般的系统（如 UNIX/Linux、Windows NT/XP、NetWare 等）都提供了对口令认证的支持，对于封闭的小型系统来说不失为一种简单可行的方法。

2．双因素认证

在双因素认证系统中，用户除了拥有口令外，还拥有系统颁发的令牌访问设备。当用户向系统登录时，用户除了输入口令外，还要输入令牌访问设备所显示的数字。该数字是不断变化的，而且与认证服务器是同步的。

3．一次口令机制

一次口令机制采用动态口令技术，是一种让用户的密码按照时间或使用次数不断动态变化、每个密码只使用一次的技术。它采用一种称为动态令牌的专用硬件，内置电源、密码生成芯片和显示屏，密码生成芯片运行专门的密码算法，根据当前时间或使用次数生成当前密码并显示在显示屏上。认证服务器采用相同的算法计算当前的有效密码。用户使用时，只需要将动态令牌上显示的当前密码输入客户端计算机，即可实现身份的确认。由于每次使用的密码必须由动态令牌来产生，只有合法用户才持有该硬件，所以只要密码验证通过就可以认为该用户的身份是可靠的。用户每次使用的密码都不相同，即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份。

4．生物特征认证

生物特征认证是指采用每个人独一无二的生物特征来验证用户身份的技术，常见的有指纹识别、视网膜识别等。理论上，生物特征认证是最可靠的身份认证方式，因为它直接使用人的生理特征来表示每一个人的数字身份，不同的人具有相同生物特征的可能性可以忽略不计，因此几乎不可能被仿冒。

5．USB Key认证

基于 USB Key 的身份认证方式是近几年发展起来的一种方便、安全、经济的身份认证技术，它采用软、硬件相结合一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。USB Key 是一种 USB 接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用 USB Key 内置的密码学算法实现对用户身份的认证。基于 USB Key 的身份认证系统主要有两种应用模式：一是基于冲击/响应的认证模式；二是基于 PKI 体系的认证模式。

8.5.3 消息认证技术

随着网络技术的发展，对网络传输过程中信息的保密性提出了更高的要求，这些要求主要包括：

（1）对敏感的文件进行加密，即使他人截取文件也无法得到其内容。

（2）保证数据的完整性，防止截获者在文件中加入其他信息。

（3）对数据和信息的来源进行验证，以确保发信人的身份。

现在，业界普遍通过加密技术方式来满足以上要求，实现消息的安全认证。消息认证就是验证所收到的消息确实是来自真正的发送方且未被修改的消息，也可以验证消息的顺序和

及时性。

消息认证实际上是对消息本身产生一个冗余的信息——MAC（消息认证码），消息认证码是利用密钥对要认证的消息产生新的数据块并对数据块加密生成的。它对于要保护的信息来说是惟一的，因此可以有效地保护消息的完整性，以及实现发送方消息的不可抵赖和不能伪造。

消息认证技术可以防止数据的伪造和被篡改，以及证实消息来源的有效性，已广泛应用于信息网络。随着密码技术与计算机计算能力的提高，消息认证码的实现方法也在不断地改进和更新，多种实现方式会为更安全的消息认证码提供保障。

8.5.4 数字签名

所谓数字签名，就是附加在数据单元上的一些数据（用私钥加密的数据），通过这些数据，接收者可以确认数据单元的来源和完整性，以防止数据被人改动或抵赖行为的发生。它是对电子形式的消息进行签名的一种方法，故称为数据签名。目前，数字签名主要基于公钥加密体制。实际上，数字签名是一个用私钥加密的信息摘要，附在消息后面，以确认发送者的身份和该信息的完整性。

数字签名有两种：一是对整体消息的签名，即消息经过密码变换后被签名的消息整体；二是对压缩消息的签名，即附加在被签名消息之后或某一特定位置上的一段签名图样。若按明文、密文的对应关系划分，每一种又分为两个子类：一类是确定性数字签名，其明文与密文一一对应，它对一特定消息的签名不变化，如 RSA 签名；另一类是随机化的或概率式数字签名，它对同一消息的签名是随机变化的，取决于签名算法中的随机参数的取值。一个明文可有多个合法的数字签名，如 ElGamal。

下面举例说明数字签名的应用。

若 A 向 B 发送消息，其创建数字签名的过程如图 8.10（a）所示。

（1）利用散列函数计算原消息的摘要。

（2）用自己的私钥加密摘要，并将摘要附在原消息的后面。

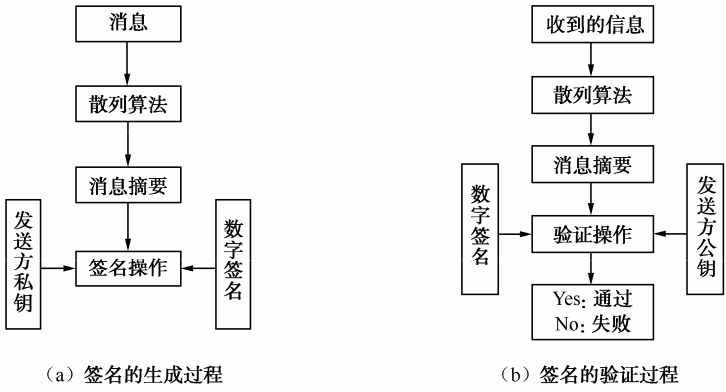
B 收到消息，对数字签名进行验证的过程如图 8.10（b）所示。

（1）将消息中的原消息及其加密后的摘要分离出来。

（2）使用 A 的公钥将加密后的摘要解密。

（3）利用散列函数重新计算原消息的摘要。

（4）将解密后的摘要与自己用相同散列算法生成的摘要进行比较。若两者相等，则说明消息在传递过程中没有被篡改；否则，消息不可信。



（a）签名的生成过程　　（b）签名的验证过程

图 8.10　数字签名

了解数字签名及其验证过程后可以发现，这一技术带来了以下三个方面的安全性。

（1）信息的完整性：由散列函数的特性可知，如果信息在传输过程中遭到篡改，B 重新计算出的摘要必然不同于用 A 的公钥解密出的摘要，因此 B 就确信信息不可信。

（2）信源确认：因为公钥和私钥之间存在对应关系，既然 B 能用 A 的公钥解开加密的摘要，并且其值与 B 重新计算出的摘要一致，那么该消息是 A 发出的。

（3）不可抵赖性：这一点实际上是（2）的理由阐述。因为只有 A 持有自己的私钥，其他人不可能冒充他的身份，所以 A 无法否认他发过这一则消息。

本 章 小 结

本章主要讲述了以下内容。

（1）网络安全是一个相对的概念，其本质是网络信息的安全问题。

（2）网络安全的特征：保密性、完整性、可用性、可控性和可审查性。网络安全的目标主要表现在可靠性、可用性、保密性、完整性上。

（3）计算机网络面临的安全威胁主要有截获、中断、篡改和伪造 4 种。

（4）计算机网络安全的内容涉及网络实体安全、网络软件安全、网络数据安全和网络安全管理等方面。

（5）计算机病毒指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

（6）按病毒感染的途径，病毒分为引导型病毒、文件型病毒和复合型病毒 3 类。

（7）蠕虫程序和特洛伊木马程序是病毒程序。

（8）对付病毒最理想的方法是预防，加强预防措施可以减少病毒攻击的成功次数。

（9）防火墙是由软件、硬件构成的系统，是一种特殊编程的路由器，用来在两个网络之间实施接入控制策略。

（10）防火墙的主要 3 种技术是包过滤、网络地址翻译和应用级代理。根据防火墙采用的技术，防火墙分为 3 种基本类型，即包过滤型、代理型和监测型。

（11）密码技术分为加密和解密两部分，密码编码学与密码分析学组合形成密码学。

（12）对称密钥体制也称为私钥密码体制，它使用相同的密钥加密和解密信息。DES 和 AES 是对称密钥体制的典型。

（13）非对称密钥体制也称为公开密钥体制，它要求密钥成对出现，一个为公共密钥，另一个为专用密钥，并且不可能从其中一个推导出另一个。非对称密钥算法中使用最广的是 RSA。

（14）数字信封是公钥密码体制在实际中的一个应用，是用加密技术来保证只有规定的特定收信人才能阅读通信的内容。

（15）认证指证实被认证对象是否属实和是否有效的一个过程。认证一般可以分为身份认证和消息认证，身份认证用于鉴别用户身份，消息认证用于保证信息的完整性和抗否认性。

（16）数字签名是附加在数据单元上的一些数据（用私钥加密的数据），通过这些数据，接收者可以确认数据单元的来源和完整性，以防止数据被人改动或抵赖行为的发生。

思 考 题

1．狭义的网络安全指的是什么？
2．网络安全主要包括哪些方面？
3．计算机网络面临的安全威胁来自哪些方面？
4．根据目前病毒的侵袭情况，请给计算机病毒下一个准确的定义。
5．防火墙依靠什么来阻止攻击？请列出你所知道的防火墙名称。
6．简述非对称密钥加密的原理。
7．什么是认证？请举出几种常用的身份认证方法。
8．什么是数字签名？数字签名起什么作用？

实训 15　防火墙的配置与管理

一、实训目的

1．了解、熟悉常见的防火墙产品。
2．掌握防火墙基本结构、安全性能指标及接口并掌握典型防火墙的主要功能。
3．了解防火墙管理方式，初步掌握防火墙用户界面的使用方法。

二、实训环境

1．接入网络的计算机至少为两台。
2．一台安装有 Windows Server 2003 的计算机。
3．正版的瑞星个人防火墙软件和端口扫描软件（X-Scan、Can-Port 等）。

三、实训内容

1．安装、设置个人防火墙。
2．根据实际情况，设置相应的安全策略。
3．掌握基本的包过滤规则设置。
4．验证规则的设置。

四、方法和步骤

1．安装瑞星个人防火墙。

（1）启动安装程序。通过网络将瑞星个人防火墙软件下载到你的计算机的指定文件夹下，找到该文件夹，双击运行瑞星个人防火墙下载版安装程序，进行防火墙的安装。这时会给出安装提示，用户只要按照相应提示，就可以轻松地进行安装。

（2）填写产品序列号和用户 ID。当出现如图 8.11 所示的“输入序列号”窗口时，在“请输入您的产品序列号”框中输入瑞星个人防火墙的产品序列号，在“请输入您的用户 ID”框中输入瑞星个人防火墙的用户 ID（12 位）。

（3）填写完产品序列号和用户 ID 后，单击“下一步”按钮，然后按照提示继续安装。

（4）安装成功。当软件安装成功后会出现结束对话框，默认是启动“瑞星个人防火墙”程序，当用户单击“完成”按钮后，就完成了整个瑞星个人防火墙的安装，这时会自动启动瑞星个人防火墙软件。（用户也可以通过打钩的方法，自行改变要启动的程序。）

图 8.11　“输入序列号”窗口

2．设置瑞星个人防火墙。

（1）启动瑞星个人防火墙。单击“开始”→“所有程序”→“瑞星个人防火墙”→“瑞星个人防火墙”，启动瑞星个人防火墙软件。

（2）启动成功后的界面。成功启动瑞星个人防火墙后的界面如图 8.12 所示，该界面的下方提示“您已处于瑞星防火墙保护之下，日志记录显示在上面的列表中”。

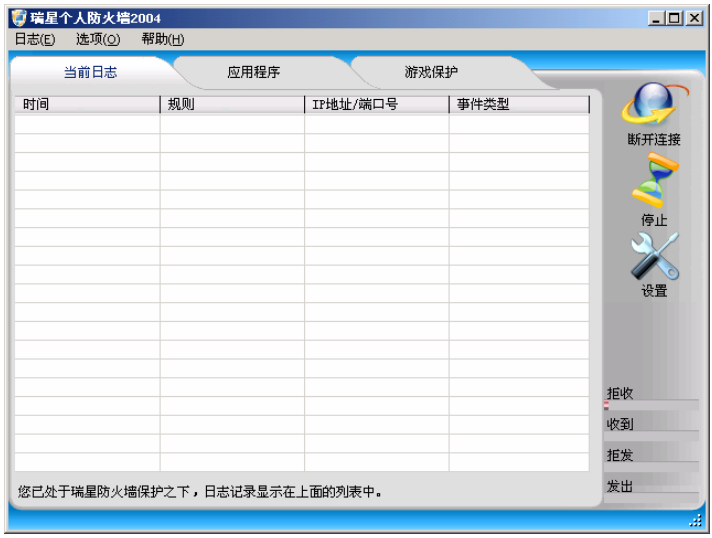


图 8.12　“瑞星个人防火墙”界面

（3）规则设置在“瑞星个人防火墙”界面中，单击“选项”→“规则设置”菜单命令，弹出如图 8.13 所示的窗口。

防火墙规则指定计算机可进行哪种形式的网络通信，用户可以通过添加、修改、删除和插入等操作来自定义防火墙规则。

（1）添加：单击“规则”→“添加”菜单命令，打开“添加防火墙规则”对话框，在该对话框中可以定义规则，从而允许、禁止特定类型的网络通信。

（2）插入：若要插入防火墙规则，请选择该规则，然后单击“规则”→“插入”菜单命令，打开“插入防火墙规则”对话框，在该对话框中可以插入一项新规则。

图 8.13　“瑞星个人防火墙规则设置”窗口

（3）修改：若要更改防火墙规则，请选择该规则，然后单击“规则”→“修改”菜单命令，打开“更改防火墙规则”对话框，在该对话框中可以更改规则的内容。

（4）删除：若要删除防火墙规则，请选择该规则，然后单击“规则”→“删除”菜单命令。

3．验证防火墙规则。

根据对瑞星个人防火墙规则设置的内容，在客户机端验证防火墙规则设置改变前后的网络使用情况。

五、实训报告要求

1．在 Windows Server 2003 默认安装条件下，打开了哪些端口？请列举 5 个。

2．总结瑞星个人防火墙规则设置的内容。

3．总结针对不同的安全策略应如何设置防火墙。

第 9 章　网络系统集成概述

本章要点

网络系统集成就是通过结构化的综合布线系统和计算机网络技术，将各个分离的设备（如个人计算机）、功能和信息等集成到相互关联的、统一和协调的系统中，使资源达到充分共享，实现集中、高效、便利的管理。本章主要讨论网络系统集成相关的这些问题。

本章目标

- 了解综合布线技术
- 理解局域网的系统集成的概念
- 了解广域网连接技术与设计方案

9.1　综合布线技术

9.1.1　综合布线技术概述

1．综合布线技术的产生与发展

早在 20 世纪 50 年代，经济发达的国家在城市中兴建新式大型高层建筑，为了增加和提高建筑的使用功能和服务水平，首先提出楼宇自动化的要求，在房屋建筑内装有各种仪表、控制装置和信号显示等设备，并采用集中控制、监视，以便于运行操作和维护管理。因此，这些设备都需分别设有独立的传输线路，将分散设置在建筑内的设备相连，组成各自独立的集中监控系统，这种线路一般称为专业布线系统。由于这些系统基本采用人工手动或初步的自动控制方式，科技水平较低，所需的设备和器材品种繁多而复杂，线路数量很大，平均长度也长，不但增加工程造价，而且不利于施工和维护。自 20 世纪 80 年代以来，随着科学技术的不断发展，尤其是通信、计算机网络、控制和图形显示技术的相互融合和发展，高层房屋建筑服务功能的增加和客观要求的提高，传统的专业布线系统已经不能满足需要。为此，发达国家开始研究和推出综合布线系统。20 世纪 80 年代后期，综合布线系统逐步引入我国。近几年来，我国国民经济持续高速发展，城市中各种新型高层建筑和现代化公共建筑不断建成，尤其是作为信息化社会象征之一的智能化建筑中的综合布线系统已成为现代化建筑工程中的热门话题，也是建筑工程和通信工程中设计和施工相结合的一项十分重要的内容。

建筑物与建筑群综合布线系统，简称为综合布线系统。它是指一幢建筑物（或综合性建筑物）内或建筑群体中的信息传输媒质系统。它将相同或相似的缆线（如对绞线、同轴电缆或光缆）、连接硬件组合成一套标准的且通用的、按一定秩序和内部关系而集成的整体，因此，目前它是以通信自动化（CA）为主的综合布线系统。今后随着科学技术的发展，它将逐步提高和完善，能真正充分满足智能化建筑所需的要求。

2．综合布线系统的特点

综合布线系统是目前国内、外推广使用的比较先进的综合布线方式，具有以下特点。

（1）兼容性好。传统的专业布线方式需要使用不同的电缆、电线、接续设备和其他器材，技术性能差别极大，难以互相通用，彼此不能兼容。综合布线系统具有综合所有系统和互相兼容的特点，采用光缆或高质量的布线部件和连接硬件，能满足不同生产厂家的终端设备传输信号的需要。

（2）灵活性、适应性强。采用传统的专业布线系统时，如需改变终端设备的位置和数量，则必须敷设新的缆线和安装新的设备，并且在施工中有可能发生传送信号中断或质量下降，增加工程投资和施工时间，因此，传统的专业布线系统的灵活性和适应性差。在综合布线系统中，任何信息点都能连接不同类型的终端设备，当设备数量和位置发生变化时，只需采用简单的插接工序，实用方便，其灵活性和适应性都强，并且节省工程投资。

（3）便于今后扩建和维护管理。综合布线系统的网络结构一般采用星形结构，各条线路自成独立系统，在改建或扩建时互相不影响。综合布线系统的所有布线部件采用积木式标准件和模块化设计。因此，部件容易更换，便于排除障碍，并且采用集中管理方式，有利于分析、检查、测试和维修，节约维护费用和提高工作效率。

（4）技术经济合理。综合布线系统的各个部分都采用高质量材料和标准化部件，并按照标准施工和严格检测，保证系统技术性能优良可靠，满足目前和今后通信需要，并且在维护管理中减少维修工作，节省管理费用。采用综合布线系统虽然初次投资较多，但从总体上看符合技术先进、经济合理的要求。

3．综合布线系统的范围

综合布线系统的范围应根据建筑工程项目的范围而定，一般有两种范围，即单幢建筑和建筑群体。单幢建筑中的综合布线系统范围，一般指在整幢建筑内敷设的管槽系统、电缆竖井、专用房间（如设备间等）、通信缆线及连接硬件等。建筑群体因建筑幢数不一、规模不同，有时可能扩大成为街坊式的范围（如高等学校校园式），其范围难以统一划分，但不论其规模如何，综合布线系统的范围除上述每幢建筑内的通信线路和其他辅助设施外，还需包括各幢建筑物之间相互连接的通信管道和线路，这时，综合布线系统较为庞大而复杂。

我国通信行业标准《大楼通信综合布线系统》（YD/T 926）的适用范围规定是跨越距离不超过 3000m、建筑总面积不超过 100 万平方米的布线区域，其人数为 50～50 万人。布线区域超出上述范围时可参照使用。上述范围是从基建工程管理的要求考虑的，与今后的业务管理和维护职责等的划分范围有可能是不同的。因此，综合布线系统的具体范围应根据网络结构、设备布置和维护办法等因素来划分。

布线系统是整个系统集成的基础。布线技术的选择和布线系统的设计直接影响着整个大楼信息系统的生命力，并将关系到大楼的未来使用效果。

9.1.2 综合布线系统的组成

综合布线系统（Premises Distribution System，PDS）是一套开放式的布线系统，可以支持几乎所有的数据、话音设备及各种通信协议；同时，由于 PDS 充分考虑了通信技术的发展，设计时有足够的技术储备，所以能充分满足用户长期的需求，应用范围十分广泛。结构化综合布线系统具有高度的灵活性，各种设备位置的改变、局域网的变化，不需重新布线，只要在配线间做适当布线调整即可满足需求。结构化综合布线系统一般划分为六个子系统，如图 9.1 所示。

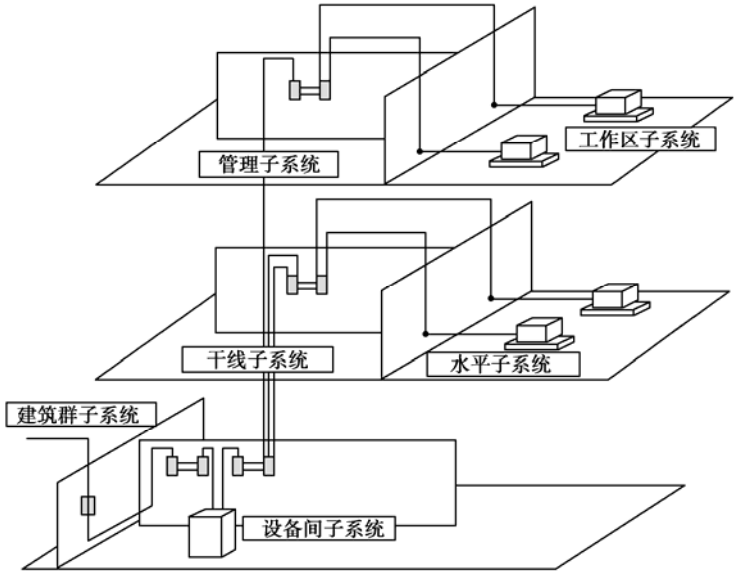


图 9.1　综合布线系统的结构

1．工作区子系统（Work Area）及其网络设计

工作区子系统由终端设备连接到信息插座的连线以及信息插座组成。信息点由标准 RJ-45 插座构成。信息点数量应根据工作区的实际功能及需求确定，并预留适当数量的冗余。例如，对于一个办公区内的每个办公点可配置 2～3 个信息点，此外应为此办公区配置 3～5 个专用信息点用于工作组服务器、网络打印机、传真机、视频会议等。若此办公区为商务应用，则信息点的传输速率为 100Mbps 可满足要求；若此办公区为技术开发应用，则每个信息点应为交换式 100Mbps 甚至是光纤信息点。

工作区的终端设备（如电话机、传真机）可用超五类或六类双绞线直接与工作区内的每一个信息插座相连接，或用适配器（如 ISDN 终端设备）、平衡/非平衡转换器进行转换连接到信息插座上。

2．水平子系统（Horizontal）及其网络设计

水平子系统主要实现信息插座和管理子系统，即中间配线架（IDF）间的连接。水平子系统指定的拓扑结构为星形拓扑。水平干线的设计包括水平子系统的传输介质与部件集成。选择水平子系统的线缆，要根据建筑物内具体信息点的类型、容量、带宽和传输速率来确定。在水平子系统中推荐采用双绞线及光纤。

在双绞线水平布线链路中，水平电缆的最大长度为 90m。若使用 100Ω UTP 双绞线作为水平子系统的线缆，可根据信息点类型的不同采用不同类型的电缆。但是，从系统的兼容性和信息点的灵活互换性角度出发，建议水平子系统采用同一种布线材料。

3．管理子系统（Administration）及其网络设计

管理子系统由交连、互连和输入/输出组成，实现配线管理，为连接其他子系统提供手段。管理子系统包括配线架、跳线设备及光纤配线架等组成设备。设计管理子系统时，必须了解线路的基本设计原理，合理配置各子系统的部件。

4．干线子系统（Backbone）及其网络设计

干线子系统指提供建筑物的主干电缆的路由，可实现主配线架与中间配线架，计算机、

PBX、控制中心与各管理子系统间的连接。干线传输电缆的设计必须既满足当前的需要，又适应今后的发展。干线子系统的布线走向应选择干线线缆最短、最安全和最经济的路由。干线子系统在系统设计施工时，应预留一定的线缆做冗余信道，这对于综合布线系统的可扩展性和可靠性来说是十分重要的。

5．设备间子系统（Equipment Room）及其网络设计

设备间子系统由设备室的电缆、连接器和相关支持硬件组成，把各种公用系统设备互连起来。设备间的主要设备有数字程控交换机、计算机网络设备、服务器、楼宇自控设备主机等。它们可以放在一起，也可分别设置。在较大型的综合布线中，可以对计算机设备、数字程控交换机、楼宇自控设备主机分别设置机房，把与综合布线密切相关的硬件设备放置在设备间，计算机网络设备的机房放在离设备间不远的位置。

6．建筑群子系统（Campus Subsystem）及其网络设计

建筑群子系统是实现建筑之间的相互连接，提供楼群之间通信设施所需的硬件。建筑群之间可以采用有线通信的手段，也可采用微波通信、无线电通信的手段。

9.1.3 综合布线系统的组网部件

综合布线系统的组网部件很多。为了方便介绍，下面以一个小型综合布线系统来加以说明。

小型的综合布线系统可以作为一个完善的智能小区综合布线系统的一部分，也可以完全独立成为一套综合布线系统，其中最具有代表性的是智能家居布线系统。从功用来说，智能家居布线系统是智能家居系统的基础，是其传输的通道。目前，国内、外大型综合布线厂家都针对智能家居市场推出了解决方案和产品。也有一些专业生产智能家居布线箱的厂家进军这一市场。

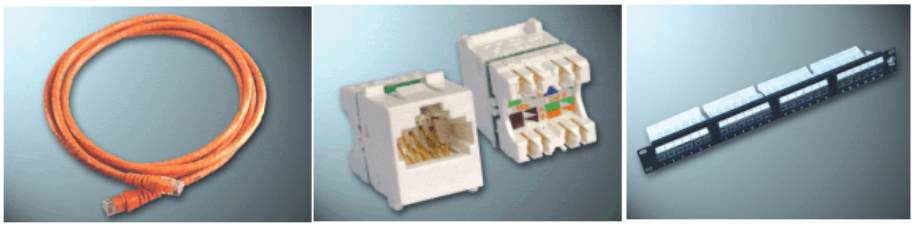
智能家居布线也要参照综合布线标准进行设计，但它的结构相对简单。智能家居布线主要参考标准为家居布线标准（TIA/EIA 570-A）草议。TIA/EIA 570-A 草议主要是制定出新一代的家居电信布线标准，现今及将来的电信服务。标准主要提出有关布线的新等级，并建立一个布线介质的基本规范及标准，主要应用支持话音、数据、影像、视频、多媒体、家居自动系统、环境管理、保安、音频、电视、探头、警报及对讲机等服务。标准主要规划于新建筑、新增加设备、一住宅及建筑群等。

目前应用较多的是实施以四个功能模块为主，包括高速数据网络模块、电话语音系统模块、有线电视网模块、音响模块。

智能家居布线系统的优点是为家庭服务，能够集中管理家庭服务的各种功能应用；支持视频、语音、数据及监控信号传输；具有高带宽、高速率；具有灵活性及高可靠性；具有兼容性及开放性；易于管理；适应网络目前及将来的发展；整齐、美观。它可带来较大的效益，包括提高住宅的竞争力；投资小，见效快；住宅小区初期的安装费用降低；智能小区的管理及运行费用降低；更舒适的环境和更现代化的生活。

智能家居布线产品可以说是智能家居中最基本的产品，许多其他智能家居系统都需基于智能家居布线系统来完成传输和配线管理，包括宽带接入系统、家庭通信系统、家庭局域网、家庭安防系统、家庭娱乐系统等。作为最终用户来说，也许不用关心布线产品生产技术指标、传输技术参数等，但一定要了解家居布线使用的综合布线系统的组网部件及综合布线系统的组网部件搭配使用方法。家居布线的综合布线系统的组网部件有双绞线（Twisted-Pair）、RJ-45

模块（Modular）、配线架（Pantch Pannel）、水晶头、面板、跳线（连接线）、光纤跳线、音频/视频线、光纤跳接箱（Optical Cross Connect）、用户小交换机、转接点（Transition）等。图 9.2 是几种常用的组网部件。



（a）光纤跳线　　（b） RJ-45 模块　　（c） 配线架

图 9.2　几种常用的组网部件

9.1.4　综合布线系统的标准

1．综合布线系统的标准概要

综合布线系统自问世以来已具有近 30 年的历史，在这期间，随着信息技术的发展，布线技术也在不断推陈出新；与之相适应，布线系统相关标准的发展也有相当长的时间。国际标准化组织 ISO，欧洲电工标准化委员会 CENELEC 和北美的工业技术标准化委员会 TIA 都在努力制定更新的标准以满足技术和市场的需求。下面列出与布线有关的部分组织与机构。

（1）ANSI（American National Standards Institute，美国国家标准学会）。

（2）BICSI（Building Industry Consulting Service International，国际建筑业咨询服务）。

（3）CCITT（Consultative Committee on International Telegraphy And Telephony，国际电报和电话咨询委员会），现在改为 ITU-TSS。

（4）EIA（Electronic Industries Association，电子工业协会）。

（5）IEC（International Electrotechnical Commission，国际电工技术委员会）。

（6）IEEE（Institute for Electrical and Electronic Engineers，美国电气与电子工程师学会）。

（7）ISO（International Standards Organization，国际标准化组织）。

这些组织都在不断努力制定更新的标准以满足技术和市场的需求。目前，我国布线行业主要参照国际标准、美洲标准、国家标准及国内行业标准。已经形成并经常使用的标准如下。

1）综合布线应符合的国际技术标准与规范

（1）《国际商用建筑物电信布线标准》EIA/TIA 568A/569A/570A/606/607。

（2）《客户建筑物电缆通用敷设要求》ISO/IEC IS 11801。

（3）《非屏蔽双绞线传输性能验收规范》EIA/TIA TSB-67/72。

（4）《电气与电子工程师学会标准》IEEE 802.3/802.5。

（5）《建筑及建筑群综合布线系统工程设计规范》（CECS 72:97）。

（6）《建筑与建筑群综合布线系统工程施工及验收规范》（CECS 89:97）。

（7）《美国国家电气规范》（NEC）。

2）综合布线所涉及的国家、行业、地方标准与规范

（1）《民用建筑电气设计标准》JGJ/TI16-92。

（2）《工业企业通信设计规范》GBJ42-81。

（3）《工业企业通信接地设计规范》GBJ79-85。

（4）《建筑与建筑群综合布线系统工程设计规范》CECS72:97。

（5）《建筑与建筑群综合布线工程施工与验收规范》CECS89:97。

（6）《Lucent 结构化布线系统设计》。

2．EIA/TIA 568 国际综合布线标准

《国际商用建筑物电信布线标准》EIA/TIA 568A/569A/570A/606/607 是计算机网络中用得很广泛的一种国际综合布线标准。

这个标准确定了一个可以支持多品种、多厂家的商业建筑的综合布线系统，同时也提供了为商业服务的电信产品的设计方向。即使对随后安装的电信产品不甚了解，该标准也有助于对产品进行设计和安装。在建筑建造和改造过程中进行布线系统的安装，比建筑落成后实施要大大节省人力、物力、财力。 这个标准确定了各种各样布线系统配置的相关元器件的性能和技术标准。为达到一个多功能的布线系统，已对大多数电信业务的性能要求进行了审核。业务的多样化及新业务的不断出现会对所需性能做某些限制。用户为了了解这些限制，应知道所需业务的标准。

这个标准是一系列关于建筑布线中电信产品和业务的技术标准之一。EIA/TIA 568 标准连同相关的标准满足了电信行业发展企业结构的需要。另外两个为电信服务的主要标准是商业建筑标准（EIA/TIA-569）（Ref B1.3）和住宅及小型商业区综合布线标准（EIA/TIA-570）（Ref B1.2）。

《国际商用建筑物电信布线标准》EIA/TIA 568A/569A/570A/606/607 分为强制性和建议性两种标准。强制性标准通常适用于保护、生产、管理、兼容，它强调了绝对的最小限度可接受的要求，建议性标准通常针对最终产品。在某种程度上，在统计范围内确保全部产品与使用的设施设备相适应体现了这些标准。另外，建议性标准用来在产品的制造中提高生产率，无论是强制性标准还是建议性标准都是同一技术规范。建议性标准是为了达到这样一个目的：未来的设计要努力达到特殊的兼容性或实施的先进性。

这个标准对于一座建筑直到包括通信插口和校园内各建筑物间的综合布线规定了最低限度的要求，它对一个带有被认可的拓扑和距离的布线系统，对以限定实施参数为依据的媒体进行了说明，并对连接器及插头引线间的布置连接也做了说明。这个标准适用于办公地点要求的商业建筑的综合布线。

9.1.5　综合布线系统的设计等级

综合布线系统应能满足所支持的语音、数据、图像系统的传输速率和标准要求，并应选用相应等级的传输电缆和设备。综合布线系统的所有设备之间的连接端子、塑料绝缘电缆或电缆扎线带都应有色标。不仅各个线对是用颜色标志的，而且各线束组也使用同一图表中的色标，以有利于维护检修。

另外，综合布线系统中的星形拓扑结构特点，可使任一子系统单独地布线，每一子系统均为一独立的单元组，更改任一子系统时，均不会影响其他子系统，这给整个布线系统设计带来极大的方便。一个设计完善的布线系统的目标是，允许在有新需求的集成过程中，不必进行水平布线、损坏建筑装饰而影响审美。为了使综合布线系统设计具体化，根据实际需要，可将综合布线系统分为以下 3 个设计等级。

1．基本型

基本型适用于综合布线系统配置标准较低的场合，用铜芯电缆组网。基本型综合布线系统的配置如下。

（1）每个工作区（站）有一个信息插座。

（2）每个工作区（站）的配线电缆均为一条独立的 4 对双绞线（通常是 5 类以上），引至楼层配线架。

（3）完全采用夹接式交接硬件（如配线架、配线箱）。

（4）每个楼层的干线电缆（楼层配线架至设备间的中心配线架电缆）至少有两对双绞线。

基本型综合布线系统是一种最经济的方案，但同样能支持绝大多数企业所需的语音和数据应用（一般没有对带宽要求过高的多媒体应用，如电视教学、可视电话等）。

2．增强型

增强型适用于综合布线系统配置标准中等的场合，也是用铜芯电缆组网。增强型综合布线系统的配置如下。

（1）每个工作区（站）有两个以上的信息插座，一方面可以用来冗余，另一方面可以用来扩展。

（2）每个工作区（站）的配线电缆均为一条独立的 4 对双绞线（通常是 5 类以上），引至楼层配线架。

（3）每个楼层的干线电缆（楼层配线架至设备间的中心配线架电缆）至少有 3 对双绞线，其中 2 对用于数据传输，1 对用于语音传输。

增强型与基础型综合布线系统相比，主要区别是提供了扩展余地，在功能上无太大区别，同样支持语音和数据应用，但它可按需要利用端子板进行管理。

3．综合型

综合型适用于综合布线系统配置标准较高的场合，采用光纤和铜芯电缆混合组网。综合型综合布线系统配置与增强型系统相比，增设了光缆系统，可适用于规模较大的建筑物或建筑群，其余特点与基本型或增强型相同。

9.1.6 综合布线系统的设计方法

设计与实现一个合理综合布线系统一般需要经过以下 6 个步骤。

（1）获取建筑物平面图：这是整个综合布线系统设计的基础，因为无论哪个子系统都直接与建筑物结构平面图息息相关。

（2）分析用户需求：具体选择哪种布线方式，哪个工作区布置多少个信息点，干线系统采用什么电缆，配线间和设备间打算安排在哪个位置等，主要取决于对用户需求的分析。

（3）布线系统结构设计：这是综合布线系统设计的开始，主要完成布线系统的总体结构设计，特别是各工作区、水平子系统的布线系统设计。

（4）布线系统路由设计：这一步完成整个布线系统中各工作区子系统通过干线子系统与设备间子系统、管理子系统的路由连接设计，以及建筑群子系统（可选）之间的路由连接设计。

（5）绘制布线施工图：这相当于综合布线系统施工的工艺图，用来指导布线人员的施工。在这个施工图中要对一些关键信息点、交接点、电缆拐点等位置的施工注意事项和布线槽（或线管）规格、材质等进行详细的标注或说明。

（6）编制用料清单：这也是用来指导具体布线施工的，因为这些材料都需要在具体布线施工中用到，对于一些特殊材料所用的位置，需要在布线图中加以说明。布线材料包括各种规格的电缆（如双绞线、光纤）、水晶头、跳线、配线架、线槽、线管等。

9.2 局域网的系统集成

9.2.1 局域网系统集成概念

所谓系统集成，就是通过结构化的综合布线系统和计算机网络技术，将各个分离的设备（如个人计算机）、功能和信息等集成到相互关联的、统一和协调的系统中，使资源达到充分共享，实现集中、高效、便利的管理。系统集成应采用功能集成、网络集成、软件界面集成等多种集成技术。系统集成实现的关键在于解决系统之间的互连和互操作性问题，它是一个多厂商、多协议和面向各种应用的体系结构。这需要解决各类设备、子系统间的接口、协议、系统平台、应用软件等与子系统、建筑环境、施工配合、组织管理和人员配备相关的面向集成的过程。

系统集成有以下几个显著特点：

（1）系统集成要以满足用户对需求为根本出发点。

（2）系统集成不是选择最好的产品的简单行为，而是要选择最适合用户的需求和投资规模的产品和技术。

（3）系统集成不是简单的设备供货，它体现更多的是设计、调试与开发，是技术含量很高的行为。

（4）系统集成包含技术、管理和商务等方面，是一项综合性的系统工程。技术是系统集成工作的核心，管理和商务活动是系统集成项目成功实施的可靠保障。

（5）性能价格比的高低是评价一个系统集成项目设计是否合理和实施成功的重要参考因素。

系统集成作为一种服务方式，是这些年来国际信息服务业中发展势头最猛的一个行业。系统集成的本质就是最优化的综合统筹设计。一个大型综合计算机网络系统的集成包括计算机软件、硬件、操作系统技术、数据库技术、网络通信技术等的集成，以及不同厂家产品选型、搭配的集成。系统集成所要达到的目标是整体性能最优，即所有部件和成分合在一起后不但能工作，而且全系统是低成本的、高效率的、性能匀称的、可扩充性和可维护的系统。为了达到此目标，系统集成商的优劣是至关重要的。

例如，一个企业，无论其规模大小，都可以根据需求从硬件方面（包括布线施工、网络接入、设备采购、网络架设、服务器架设、甚至电话系统和监控系统的架设）和软件方面（提供网络设计方案、网站架设、软件采购与售后服务、网络设备和计算机的设置、故障排除、VPN 等）进行设计。

一般中型商务企业需要企业网（Intranet）、企业信息系统、共享打印机、共享 Internet 接入。企业应当拥有一个稳定的网络平台，接入这个系统的设备，一般是采用 100Mbps 全双工的交换机、服务器和客户机。同时，需合理地划分 VLAN，可以有效地控制网络广播，减轻网络传输的负担，通过交换机的公共端口，提供不同 VLAN 之间的高效通信；通过授权对安全隔离加以控制。当然，还要考虑接入 Internet 和远程用户接入。具体方案如图 9.3 所示。

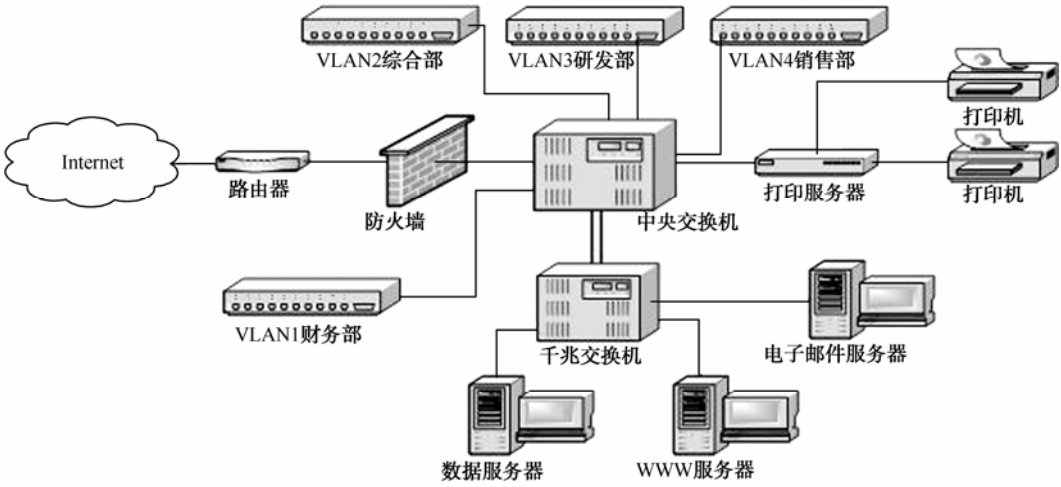


图 9.3　一般中型商务企业网络方案

系统集成项目是一项综合性的系统工程，因此，系统集成项目人员应该深刻理解项目管理中的基本概念，能运用项目管理中的知识指导自己的项目。

一名合格的系统集成工程师一般应具备以下素质。

（1）通晓计算机及网络基础理论，只有熟悉、掌握了理论和技术，才能正确、合理地设计网络系统，完整地进行系统实施。

（2）精通网络设备调试技术、服务器调试技术、基础应用平台调试技术或其中之一。掌握一种售后调试技术，是系统集成工程师必备的技能。

（3）精通网络平台设计、服务器设计、基础应用平台设计等或其中之一。能够设计相应的网络系统和应用系统，是售前技能掌握情况的重要指标。

（4）良好的语言表达能力和文字表达能力。在系统集成实施的各个阶段中，在与用户交流、方案与标书撰写、投标与答疑、用户培训和竣工文档编写等工作中，写作能力与口才是重要的基本素质。

（5）较高的计算机专业英语水平。在系统集成中，英语随处可见，在产品介绍、产品配置与报价、产品技术文档、培训等资料方面，英语都是主要文字之一。越是高端的产品，英语使用得越普遍。有时，还需要英语听说能力，而在国际招标项目中，英文写作能力将受到考验。

（6）良好的人际交流能力和与他人协同工作的能力。系统集成是一项需多人合作共同完成的系统工程，与同事、供货商、用户、厂商、施工队等的交流、合作必不可少。系统集成工程师应是一个善于与人沟通、善于与人建立良好关系的人。

（7）在压力环境下现场解决问题的能力。系统集成的技术工作往往是紧张忙碌的，尤其是在用户现场安装调试或售后故障维修时遇到技术难题的情况下，现场可用资源很少，打电话寻求支援又不方便，更有一旁用户审视的目光，这种环境是对工程师智商、情商、技术水平和调试经验的综合考验。

（8）广博的知识面。系统集成涵盖的范围很广，工程师应该一专多能、一精多通，这样，在与用户交流时就会游刃有余，避免出现用户的话题稍一偏离项目主题就茫然不知的尴尬局面。

9.2.2　局域网与结构化布线技术

局域网按照其规模可以分为大型局域网、中型局域网和小型局域网三种。不同的局域网，涉及的结构化布线技术也不相同。

1．小型局域网

小型局域网主要用于实现网内用户的全部信息资源共享，例如实现文件共享、打印共享、收发电子邮件、Web 发布、财务管理以及人事管理等功能。由于此类局域网往往接入的计算机节点比较少，一般为 20～50 台，而且各节点相对集中，每个站点与集线器或交换机之间的距离不超过 100m，采用双绞线进行结构化布线就足够了。

在选用硬件方面，由于交换机十分强调端口交换能力，内置交换模块，性能比集线器高很多，采用交换机可以提高整个网络的性能；因为现在的低端桌面交换机价格比较便宜，与集线器相比价格略高少许，所以可以采用桌面交换机。

此外，由于现在 10/100Mbps 自适应网卡与 10Mbps 网卡价位相差无几，因此所有计算机（包括服务器和 PC）都可以选用 10/100Mbps 自适应网卡，如果交换机端口不够，可以考虑采用 PC 通过集线器相连然后接入交换机。

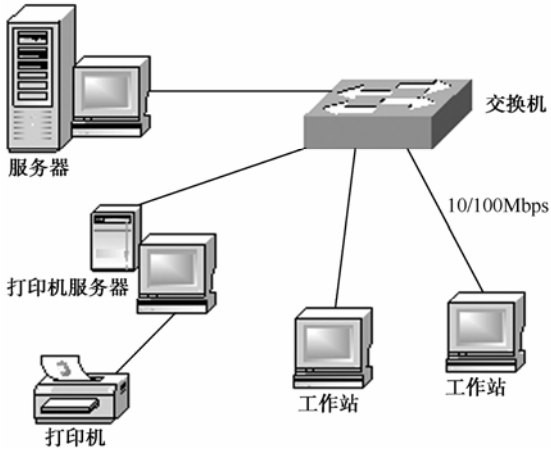


图 9.4　小型局域网模型

考虑到更好的电磁特性和将来的可升级性，所有的连线均采用 UTP5 类或超 5 类线，并且严格按照 EIA/TIA 568 规范进行综合布线。综合布线不仅使办公环境整洁，更重要的是规范、可靠安全。由于在设计网络时采用了桌面交换机，所以网络传输速率比较快，能适应高速网络的发展，并且升级容易。

2．中型局域网

中型局域网需要连接的计算机节点一般都在 60 台以上，并且各节点之间的距离也较远，一般都会超过 100m 甚至更远，利用双绞线作为传输介质已经远远不够。此时，企业办公环境对网络的性能要求较高，对网络的传输速度也有一定的要求，相对来讲，企业往往有较多的资金投入，可以使用光纤介质来连接整个企业园区的主干网络，因为光纤的有效传输距离可以达到 2km（多模光纤）或更长（单模光纤）。

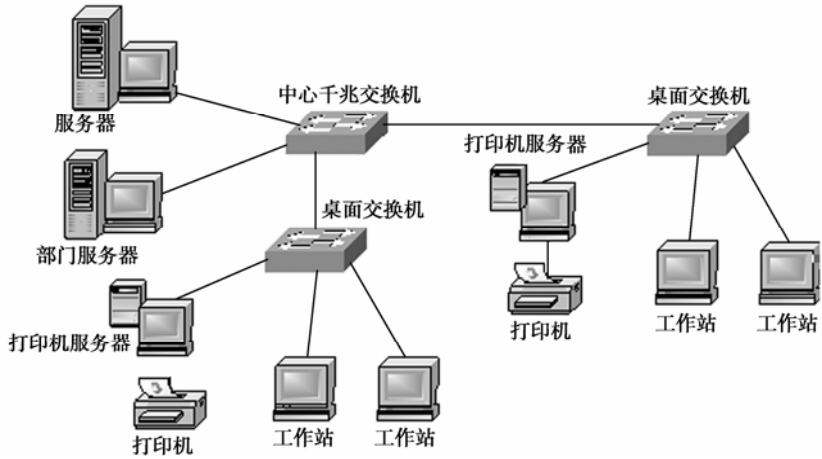


图 9.5　中型局域网模型

中型局域网可以采用两层结构，即中心交换机层和供各个节点连入的桌面交换机层。中心交换机可以采用一台高档的企业级交换机，提供多个千兆网络端口。各个节点的桌面交换机连接到中心交换机上，这些桌面交换机内部就相当于一个小型局域网。

中心服务器为了适应整体性能要求，采用千兆服务器网卡。这种方案需要大量的资金，不过相对于企业来说，可以提供优质的服务和得到较高的数据传送速度，性价比（性能价格比）比较高。

中型局域网可采用拥有 2 个端口的非网管千兆交换机，将 2 个千兆接口中的一个连接服务器，另一个接口与其他交换机建立千兆连接，充分满足中、小企业对带宽的需求。用户接入部分可通过级联 10/100Mbps 自适应交换机来增加端口用户数量。该方案的特点是性价比高，即插即用，无需进行配置。

3．大型局域网

大型的企业局域网的覆盖范围极广。

因此，必须采用性能优良、功能强大的设备才能保证整个系统稳定、安全、可靠地运行。

建造大型局域网时需要考虑的因素很多，可分为总体局域网络的建设、部门局域网的组织、Internet 的接入系统、远程广域网的实施等几个部分。

需要大型局域网的企业一般都把高性能的网络通信作为性能需求的第一位，这种大型局域网应该采用千兆以太网，中心交换机可选用企业级高密度中心交换机。适宜采用两层结构或者三层结构。

这两种方案的选择应该视具体情况而定，如果整个局域网比较分散，部分节点比较集中，则应采用三层结构。如果各个节点都比较分散，桌面交换机连接到骨干交换机上路程较远，则应采用两层结构。当然，也可以采用两层结构和三层结构混合的方法，把相对集中的桌面交换机通过骨干交换机汇集起来连接到中心交换机，将分散的节点直接连接到中心交换机。

在确定局域网的规模后，就要按照局域网中各个节点的位置、系统的复杂程度以及网络实现的功能来确定局域网的连接方式。

一般来说，企业和公司局域网常用的连接方式有集中式网络连接和分布式网络连接两种。

大多数中、小企业都采用较为集中的办公方式，即所有部门和人员都在同一座建筑内办公。由于网络的整体规模有限，局域网的覆盖范围不广，所以比较适合采用集中式网络，如

星形网和总线形网。集中式中、小型办公网中各个节点之间的连接距离通常小于 100m，因此可以全部采用 5 类 UTP 双绞线进行布线，集中式网络通常包括网络中心和楼层设备间的两层结构。典型的集中式企业网络应用范例如图 9.6 所示。

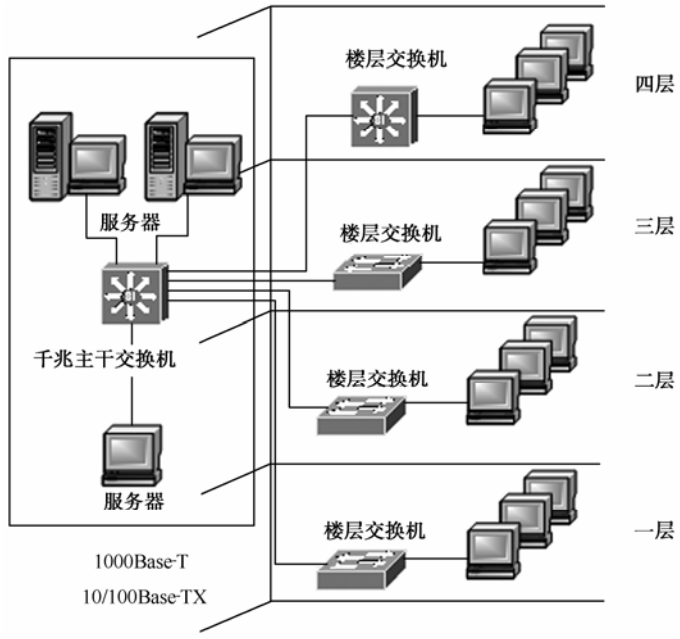


图 9.6　典型的集中式企业网络应用范例

网络中心交换机可采用千兆交换技术构成高速骨干网，用以连接服务器与楼层接入设备。中心交换机应具有大容量的交换背板，采用模块化机箱设计，可以支持多种速率和传输介质，而且端口密度高且扩展灵活。

楼层接入交换机应具有千兆端口，能够通过堆叠或增加模块来提高接入端口的密度，还应支持 SNNP 等网管协议，以便通过网络对所有设备的状况进行监控和管理。

分布式办公是指企业在一个较大的范围内具有多处办公地点，适合采用分布式网络连接方式。由于各个办公点间的连接距离通常大于 100m，所以需要采用同轴电缆或光纤进行布线。分布式网络通常具有网络中心及楼宇接入节点两个层次。如果楼宇规模较大，还可能出现第三个层次——楼层间接入设备。

采用分布式网络方案（如图 9.7 所示）的企业，各部门往往分别位于不同的建筑中，因各建筑与网络中心之间的距离大于 100m，故采用基于多模光纤传输的 1000Base-SX（多模光纤千兆以太网技术）建立千兆主干网。

中心千兆交换机可安装 100/1000Base-T（双绞线千兆以太网技术）千兆铜缆模块以连接服务器，另需选配 1000Base-SX 模块以连接其他建筑，还可选配 10/100Base-TX（双绞线快速以太网技术）模块实现该建筑内的接入。该方案采用光纤网络扩大网络覆盖范围，如果连接超过 550m，则可选用单模 1000Base-LX 长波千兆光纤技术实现 5km 内的连接。

此外，对于一些实时性较强的网络环境，如金融、证券、电子商务等企业的局域网，对网络连接的可靠性和稳定性要求很高。此时，可以采用生成树、端口聚合等技术，而中心交换机还可以用双电源冗余的方式来提高安全性。当主链路发生故障时，便可以自动接通备份

链路，以确保网络正常工作。

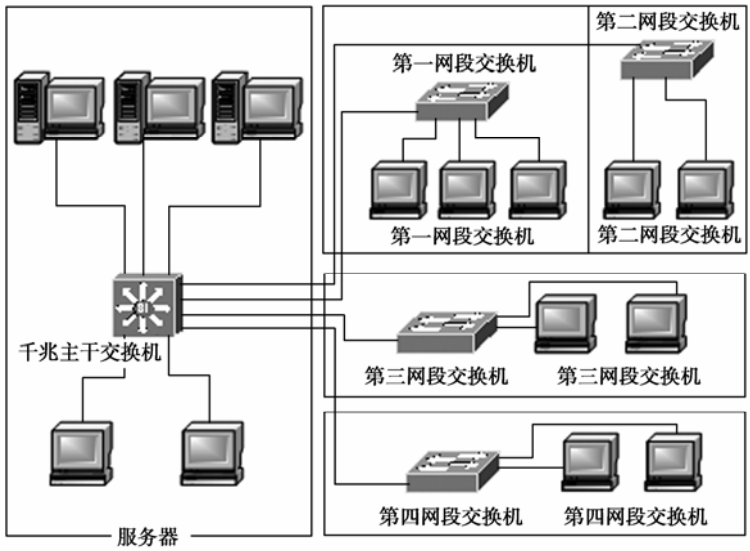


图 9.7　分布式网络方案

端口聚合可以将多条链路聚合为一组干路，还可以提高网络带宽；更重要的是，端口聚合可以实现负载均衡，从而大大提高网络的可靠性。

例如，某企业目前总共约有 60 多台计算机，分散在几个楼层、若干个办公室里，估计在组建局域网后，公司的计算机总数量会达到 100 台左右。

根据这个情况分析，10/100Mbps 的传输速率对于用户数量在 300 个以下、网络规模较小、网络应用主要以 Web 浏览、E-mail 收发、文件共享等为主的局域网来说已经是绰绰有余了。因此，应选择百兆以太网。

至于其他设备，以覆盖三层楼面的办公网为例，每一层都由一台 24 口的交换机将办公区里的十几台计算机连接起来。公司局域网示意图如图 9.8 所示。

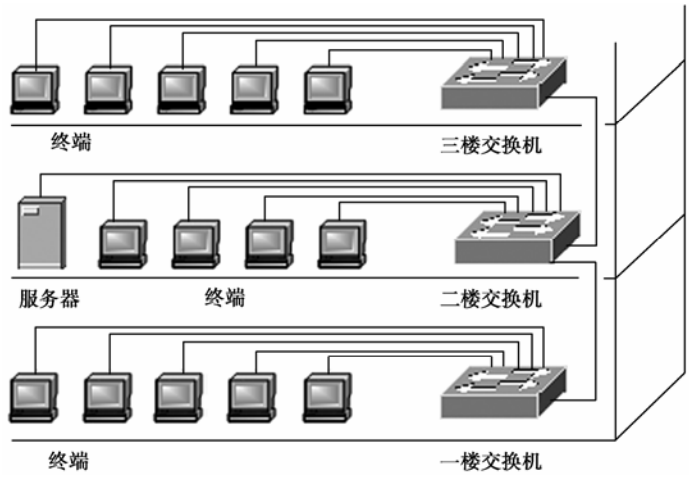


图 9.8　公司局域网示意图

考虑到更好的电磁特性和可升级性，所有的连线均采用 5 类 UTP 双绞线或超 5 类双绞线，并且严格按照 EIA/TIA 568 规范进行综合布线，以保证网络的规范性、可靠性和安全性。

交换机可以说是该网络结构中的核心设备，这里可以使用 10/100Mbps 以太网和快速以太网自适应双速交换机。它能自由地工作在 10/100Mbps 速率下，不需要配置特殊的管理软件。

以双速交换机为骨干建立起来的小型办公网，对个人通信量不大的客户机可以配置 10/100Mbps 网卡，而服务器为了更好地响应多用户的请求，宜配置高性能的 100Mbps 以太网卡。可见，这样的网络解决方案有一定的弹性，而且使用效率较高。

4．确定网络的建设成本

在确定网络的结构后，就可以初步确定建设成本。在网络规划中，网络建设的成本是一个不容忽视的问题，因为各个公司投入网络建设和管理的资金有限，所以尽可能地细化项目是很必要的。

对于交换机、防火墙、布线，其中包括水晶头、网线、配线架、机柜和信息插座等硬件购置费用，服务器、PC 以及打印机等设备的价格，加上系统的集成费用，都必须作为整个网络建设所需的资金，进行很好的预算。

总之，必须在有限的资金范围内，规划、设计、建设好企业的局域网。

9.3 广域网连接技术与设计方案

在组建广域网时，应根据用户需求和相关环境等因素，选择合适的广域网连接技术和设备。

1．广域网技术选择

目前，可以作为广域网线路通信服务的方式很多，主要有第 6 章介绍的 DDN、ISDN、Frame Relay、X.25、ADSL 等多种方式。

广域网传送数据通常使用的是公共通信链路，利用公共载波提供的条件进行传输，如由本地或长途电话公司提供的电话主干网。广域网可能要连接多个地理位置。这些单个的地理位置就是广域网节点。一个广域网链接就是两个节点之间的一个连接，连接采用的交换技术有点对点链路交换、电路交换技术、包交换技术、虚电路技术等。

广域网所利用的传输资源有公共电话交换网、同步光纤网络、无线载波技术、卫星通信网络、微波专线等。

广域网路由协议也有很多种。在一个大型的广域网中，路由协议的选择主要取决于两个方面：一是广域网的拓扑结构，二是路由协议的效率。

2．设备选型

在广域网环境中可以使用多种不同的网络设备和网络传输协议。下面着重介绍较常用的广域网设备和网络传输协议。

1）调制解调器（MODEM）

调制解调器将数字信号转换成线路要求的信号，或者把从线路上接收的信号经解调后还原成数字信号，传送给计算机。这种过程称为调制解调过程。

按通信方式可以划分，有异步 MODEM 和同步 MODEM；按使用线路划分，有拨号 MODEM、专线 MODEM、电力线 MODEM、Cable MODEM、无线 MODEM 等。

2）路由器

路由器是一种连接多个网络或网段的网络设备，是一种用于网络连接、执行路由选择任务的专用计算机。

3）CSU/DSU

信道服务单元（Channel Service Unit，CSU）/数据服务单元（Data [or Digital] Service Unit，DSU）是一个形如外置式调制解调器大小的硬件设备。

它可以提供以下方面的功能：信号再生、线路调节、误码纠正、信号管理、同步和电路测试等。

4）广域网交换机

广域网交换机是在运营商网络中使用的多端口网络互连设备。

广域网（WAN）交换机能够实现 IP、无线及话音包等多种服务，在公共的帧中继、ATM 或 MPLS（多协议标签交换）基础结构上有效地结合了数据、话音和视频。压缩、静音抑制和其他功能最大限度地利用带宽，而没有降低话音质量。

5）网关

网关，又称为协议转换器，可以支持不同协议之间的转换， 实现不同协议网络之间的互连。

6）接入服务器（简称NAS）

它是位于公用电话网（PSTN/ISDN）与 IP 网之间的一种远程访问接入设备。接入服务器是广域网中拨入和拨出连接的会聚点。

本 章 小 结

（1）网络系统集成就是通过结构化的综合布线系统和计算机网络技术，将各个分离的设备（如个人计算机）、功能和信息等集成到相互关联的、统一和协调的系统中，使资源达到充分共享，实现集中、高效、便利的管理。

（2）建筑物与建筑群综合布线系统，简称综合布线系统。它是指在一幢建筑物（或综合性建筑物）内或建筑群体中的信息传输媒质系统。它将相同或相似的缆线（如对绞线、同轴电缆或光缆）、连接硬件组合成一套标准的且通用的、按一定秩序和内部关系而集成的整体。

（3）结构化综合布线一般划分为工作区子系统、水平子系统、管理子系统、干线子系统、设备间子系统、建筑群子系统六个子系统。

（4）综合布线系统标准有包括 ISO 等在内的国际著名的标准化组织制定的一些标准。

（5）系统集成作为一种服务方式，是这些年来在国际信息服务业中发展势头最猛的一个行业。系统集成的本质就是最优化的综合统筹设计。一个大型综合计算机网络系统集成包括计算机软件、硬件、操作系统技术、数据库技术、网络通信技术等的集成，以及不同厂家产品选型，搭配的集成，系统集成所要达到的目标是整体性能最优。

思 考 题

一、思考题

1．简述综合布线系统的基本概念。

2．综合布线与传统网络工程布线相比，有哪些优点？

3．综合布线系统由哪几部分组成？

4．工作区子系统的组成及功能是什么？

5．水平子系统可选用哪几种线缆？

6．概述建筑群子系统的实现。

7．典型的广域网技术有哪些？

8．主要的广域网设备是什么？

二、选择题

1．发展综合布线系统主要是因为传统布线系统（　　）。

A．传输速度　　B．传输协议单一　　C．传输介质昂贵　　D．各系统互不兼容

2．与综合布线系统相关的国际标准是（　　）。

A．EIA/TIA 568　B．ISO/IEC 11810　　C．EIA/TIA 567　　D．ISO/OSI 348

3．综合布线系统常用介质是（　　）。

A．电话线　　B．同轴电缆　　C．微波传输　　D．双绞线

4．3 类 UTP 的传输速率可支持（　　）。

A．1Mbps　　B．2.5Mbps　　C．10Mbps　　D．100Mbps

5．综合布线系统的信息插座其接口采用（　　）。

A．RJ-11　　B．RJ-45　　C．RS-232　　D．RS-485

6．水平布线系统是结构化布线系统中的 6 个子系统之一，下面关于水平布线系统的说法中，错误的是（　　）。

A．将垂直布线的干线线路延伸到用户工作区的通信插座

B．水平布线系统起着支线的作用，一端连接用户工作区，另一端连接垂直布线系统或设备间

C．水平布线系统包括了用于连接用户设备的各种信息插座及相关配件（软线、连接器等）

D．在一个多层的建筑物中，水平布线系统是整个结构化布线系统的骨干部分

7．10Base-5 以太网的单网段最大长度为（　　）。

A．100m　　B．185m　　C．500m　　D．205m

8．在一般局域网中，最常用的传输介质是（　　）。

A．微波　　B．屏蔽双绞线　　C．非屏蔽双绞线　　D．光纤

9．配线架主要用于结构化布线系统的（　　）。

A．垂直干线子系统　　B．水平干线子系统

C．设备间子系统　　D．管理子系统

10．（　　）是整个结构化布线系统的骨干部分。

A．垂直干线子系统　　B．水平干线子系统

C．设备间子系统　　D．管理子系统

第 10 章　网络工程设计实例

本章要点

计算机网络工程是在信息工程方法和完善的组织机构的指导下，根据网络应用的需要，按照计算机网络系统的标准、规范和技术、详细规划和设计可行方案，将计算机网络硬件和设备、软件和技术系统性地集成在一起，成为满足用户需求、高性价比的计算机网络系统的组建过程。

本章讲述了计算机网络工程的一般概念、并在此基础上对网络需求分析、网络设计的一般原则做了必要介绍，最后通过一个实例说明网络工程设计与实现的过程。

本章目标

- 了解网络工程的一般概念
- 理解需求分析的意义和方法
- 了解计算机网络的建设原则

10.1　网络工程的一般概念

网络工程是一项系统工程，涉及系统论、控制论、管理学、计算机技术、网络技术、软件工程等多个领域。网络工程是指按计划进行的网络综合性工作。它包括需求分析、系统设计、网络管理，组网等内容。计算机网络工程是网络工程的一个子概念。为简单起见，这里所说的网络主要是指计算机网络。

以分组交换 技术为核心的计算机网络，自 20 世纪 70 年代以来得到了飞速发展。采用TCP/IP体系结构的Internet得到广泛使用。

为了使得网络能够适应基于网络的多种服务在带宽、可扩缩性和可靠性等方面不断增长的需求，网络工程必须应付这些挑战，解决好网络的设计、实施和维护等一系列 技术问题。作为一门学科，网络工程必须总结并研究与网络设计、实施、维护有关的概念和客观规律，能够根据这些概念和规律来设计和建造满足客户需求且跟得上Internet发展步伐的计算机网络。

计算机网络工程主要包含以下要素：

（1）明确的网络应用需求、网络业务和网络功能。

（2）有具体的规划设计方案和实施规范。

（3）有完善的组织机构、工程设计人员和工程管理人员。

（4）工程设计人员要全面了解计算机网络的原理、技术、协议、安全、系统布线的基本知识、发展现状和发展趋势，掌握网络应用开发技术、网站设计和 Web 制作技术、信息发布技术等。

（5）总体设计人员要掌握网络规划和设计的步骤、要点、流程、案例、技术设备选型和发展方向。

（6）工程主管人员要懂得网络工程的组织和施工过程，能把握网络工程的评审、监理、验收等环节。

综上所述，可以认为，计算机网络工程是在信息工程方法和完善的组织机构的指导下，根据网络应用的需要，按照计算机网络系统的标准、规范和技术、详细规划和设计可行方案，将计算机网络硬件和设备、软件和技术系统性地集成在一起，成为满足用户需求、高性价比的计算机网络系统的组建过程。

根据计算机网络系统的这个描述性定义，将计算机网络的内容和目标概括为如下方面。

（1）需求分析：主要分析用户现状和项目集成需求，明确网络应用需求、网络业务和网络功能。

（2）网络规划和设计：对计划建设的网络系统的类型、体系结构、硬件和软件、管理和安全等方面提出一套完整的技术方案和实施方案。

（3）软件、硬件系统的建设：主要包括计算机设备、网络设备、布线系统、网络操作系统和通信协议、数据库管理系统、网络应用软件和开发工具等。

（4）网络安全管理建设：主要包括网络管理、安全体系以及相应的软件系统的组建。

10.2 需求分析

10.2.1 需求分析的内容

需求调查的关键是与客户的沟通，要使客户满意。

需求分析找出“需”和“求”的关系，从当前业务中找出最需要重视的方面，从已经运行的网络中找出最需要改进的地方，满足客户提出的各种合理要求，依据客户要求修改已经成形的方案。

1．应用背景需求分析

应用背景需求分析概括了当前网络应用的技术背景，介绍了行业应用的方向和技术趋势，说明了本企业网络信息化的必然性。

应用背景需求分析要回答一些为什么要实施网络集成的问题。

（1）国外同行业的信息化程度以及取得哪些成效？

（2）国内同行业的信息化趋势如何？

（3）本企业信息化的目的是什么？

（4）本企业拟采用的信息化步骤如何？

2．业务需求分析

业务需求分析的目标是明确企业的业务类型、应用系统软件种类以及它们对网络功能指标（如带宽、服务质量 QoS）的要求。

业务需求分析是企业建网中首要的环节，是进行网络规划与设计的基本依据。

通过业务需求分析要为以下方面提供决策依据：

（1）需实现或改进的网络功能有哪些？

（2）需要集成的应用有哪些？

（3）需要电子邮件服务吗？

（4）需要 Web 服务吗？

（5）需要上网吗？带宽是多少？

（6）需要视频服务吗？

（7）需要什么样的数据共享模式？

（8）需要多大的带宽范围？

（9）计划投入的资金规模是多少？

3．网络管理的需求分析

网络管理是建网不可或缺的方面，网络是否按照设计目标提供稳定的服务主要依靠有效的网络管理。高效的管理策略能提高网络的运营效率，在建网之初就应该重视这些策略。

网络管理的需求分析要回答以下类似的问题。

（1）是否需要对网络进行远程管理？远程管理可以帮助网络管理员利用远程控制软件管理网络设备，使网管工作更方便、更高效。

（2）谁来负责网络管理？需要哪些管理功能？如需不需要计费，是否要为网络建立域？选择什么样的域模式？等等。

（3）选择哪个供应商的网管软件？是否有详细的评估？

（4）选择哪个供应商的网络设备？其可管理性如何？

（5）是否需要跟踪和分析处理网络运行信息？

（6）将网管控制台配置在何处？

（7）是否采用了易于管理的设备和布线方式？

4．安全性需求分析

安全性需求分析要明确以下内容。

（1）敏感性数据的安全级别及其分布情况。

（2）网络用户的安全级别及其权限。

（3）可能存在的安全漏洞，这些漏洞对本系统的影响程度。

（4）网络设备的安全功能要求。

（5）网络系统软件的安全评估。

（6）应用系统安全要求。

（7）采用什么样的杀毒软件。

（8）采用什么样的防火墙技术方案。

（9）安全软件系统的评估。

（10）网络遵循的安全规范和达到的安全级别。

5．通信量需求分析

通信量需求分析是从网络应用出发，对当前技术条件下可以提供的网络带宽做出如下评估。

（1）未来是否有对高带宽服务的要求？

（2）是否需要宽带接入方式？本地能够提供的宽带接入方式有哪些？

（3）哪些用户经常对网络访问有特殊的要求？如行政人员经常要访问 OA 服务器，销售人员经常要访问 ERP 数据库等。

（4）哪些用户需要经常访问 Internet？如客户服务人员经常要收发 E-mail。

（5）哪些服务器有较大的连接数？

（6）哪些网络设备能提供合适的带宽且性价比较高？

（7）需要使用什么样的传输介质？

（8）服务器和网络应用能够支持负载均衡吗？

6．扩展性分析

网络的扩展性有两层含义：一是新的部门能够简单地接入现有网络，二是新的应用能够无缝地在现有网络上运行。

扩展性分析要明确以下指标：

（1）企业需求的新增长点有哪些？

（2）已有的网络设备和计算机资源有哪些？

（3）哪些设备需要淘汰？哪些设备可以保留？

（4）网络节点和布线的预留比率是多少？

（5）哪些设备便于网络扩展？

（6）主机设备的升级性能如何？

（7）操作系统平台的升级性能如何？

7．网络环境需求

网络环境需求是对企业的地理环境和人文布局进行实地勘察以确定网络规模、地理分划，以便在拓扑结构设计和结构化综合布线设计中做出决策。

网络环境需求分析需要明确下列指标：

（1）园区内的建筑群位置。

（2）建筑物内的弱电井位置、配电房位置等。

（3）各部分办公区的分布情况。

（4）各工作区内的信息点数目和布线规模。

10.2.2 获得需求信息的方法

1．实地考察

实地考察是工程设计人员获得第一手资料采用的最直接的方法，也是必需的步骤。

2．用户访谈

用户访谈要求工程设计人员与招标单位的负责人通过面谈、电话交谈、电子邮件等通信方式以一问一答的形式获得需求信息。

3．问卷调查

问卷调查通常对数量较多的最终用户提出，询问其对将要建设的网络应用的要求。

10.2.3 可行性论证

通过各种途径获取的需求信息通常是零散的、无序的，而且并非所有需求信息都是必要的或当前可以实现的，只有对当前系统总体设计有帮助的需求信息才应该保留下来。

需求分析所取得的资料经过整理后得到需求分析文档，但这种需求分析文档还需要经过论证后才能最终确定下来。参与论证活动的人员除了需求分析工作的负责人外，还要邀请其他部门的负责人，以及招标方的领导和专家。

可行性论证是就工程的背景、意义、目的、目标、工程的功能、范围、需求、可选择的技术方案、设计要点、建设进度、工程组织、监理、经费等方面做出可行性验证，指出工程建设中选择软、硬件的依据，降低项目建设的总体风险。

在编写可行性论证报告时，主要对下列项目逐条加以说明：

（1）系统建设的目的。
（2）技术可行性。
（3）应用可行性。
（4）人员、资金可行性。
（5）设备可行性。
（6）安全可行性。

10.2.4 工程招标和投标

为了保证网络工程的建设质量，网络建设方应该以公开招标的方式确定承建商。参与投标的承建商拿出各自的标书参与投标，其中标书的主要内容来自于需求分析报告和可行性论证报告。

工程招投标是一个规范的网络工程所必需的环节。

（1）招标方聘请监理部门工作人员，根据需求分析阶段提交的网络系统集成方案，编制网络工程标底。

（2）做好招标工作的前期准备，编制招标文件。

（3）发布招标通告或邀请函，负责对有关网络工程问题进行咨询。

（4）接受投标单位递送的标书。

（5）对投标单位资格、企业资质等进行审查。审查内容包括企业注册资金、网络系统集成工程案例、技术人员配置、各种网络代理资格属实情况、各种网络资质证书的属实情况。

（6）邀请计算机专家、网络专家组成评标委员会。

（7）开标，公开招标各方资料，准备评标。

（8）评标，邀请具有评标资质的专家参与评标，对参评方各项条件公平打分，选择得分最高的系统集成商。

（9）中标，公告中标方，并与中标方签订正式工程合同。

计算机网络工程招标的目的是，以公开、公平、公正的原则和方式，从众多系统集成商中，选择一个有合格资质并能为用户提供最佳性能价格比的集成商。

投标人在索取、购买标书后，应该仔细阅读标书的投标要求及投标须知，在同意并遵循招标文件的各项规定和要求的前提下，提出自己的投标文件。

10.3 网络建设原则

在系统建设中，网络系统建设将遵循以下原则进行系统的规划、分析、设计、开发、维护和项目的管理。

1．先进性原则

采用当今国内、外最先进和成熟的计算机软硬件技术，使新建立的系统能够最大限度地适应今后技术发展变化和业务发展变化的需要。从目前国内发展来看，系统总体设计的先进性原则主要体现在采用的系统结构应当是先进的、开放的体系结构；采用的计算机技术应当是先进的，如双机热备份技术、双机互为备份技术、共享阵列盘技术、容错技术、RAID 技术等集成技术、多媒体技术；采用先进的网络技术，如网络交换技术、网管技术，通过智能化的网络设备及网管软件实现对计算机网络系统的有效管理与控制，实时监控网络运行情况，

及时排除网络故障，及时调整和平衡网上信息流量。

2．实用性原则

实用性就是能够最大限度地满足实际工作要求，是每个信息系统在建设过程中必须考虑的一种系统性能，它是自动化系统对用户的最基本的承诺。从实际应用的角度来看，这个性能更加重要，可以提高办公自动化和管理信息系统中系统的实用性。

3．可扩充性、可维护性原则

根据软件工程的理论，系统维护在整个软件的生命周期中所占比重是最大的，因此，提高系统的可扩充性和可维护性是提高管理信息系统性能的必备手段。

4．安全保密性原则

在一个用户的数据中，有相当一部分数据是该用户的秘密，尤其是教育行业的一些机要文件、学生档案等，是十分重要的数据，因此安全保密性对办公自动化系统显得尤其重要，系统的总体设计必须充分考虑这一点。服务器操作系统平台最好基于 UNIX、NT、OS2 等，数据库可以选 Informix、Oracle、Sybase、DB2 等，这样可以使系统处于 C2 安全级基础之上。采用操作权限控制、设备钥匙、密码控制、系统日志监督、数据更新严格凭证等多种手段可防止系统数据被窃取和篡改。

5．可靠性原则

一个中、大型计算机系统每天处理的数据量一般都较大，系统每个时刻都要采集大量的数据并进行处理，因此，任一时刻的系统故障都有可能给用户带来不可估量的损失，这就要求系统具有高度的可靠性。

6．经济性原则

在满足系统需求的前提下，应尽可能选用价格便宜的设备，以便节省投资，即选用性价比高的设备。总之，以最低成本来完成计算机网络的建设。

10.4　某学院校园网建设实例

作为学校信息化工程的基础，校园网为学校教学、科研以及综合信息服务提供了宽带多媒体网络，实现了教学科研、管理和通信的信息化应用。特别是现在，很多学校在学生逐年增多、教学任务加大、办公业务量和信息量大规模增长的同时，迫切需要建设一个高宽带、多业务处理能力、具有交互功能的校园网，以实现多媒体课件制作、多媒体教学、电子阅览等教学科研工作，使教务、行政和总务管理更有效率，满足校内外的通信要求，使数据传输、信息交流变得更为顺畅，从而整体提高校园网的综合业务处理能力。

校园网建设的主要内容如下。

（1）主干网：提供校园内计算机主干通信服务，应具有较高通信带宽和稳定可靠的特点。

（2）子主干网：作为楼宇内或协同工作的计算机集合的网络系统而提供的网络互连服务。

（3）远程办公室网：僻远工作点的网络互连。

（4）远程个人入网：对教师、科研人员、校领导或其他个人办公地点提供的网络服务。

（5）广域网连接：使校园网可以实现国内、外的信息传输。这是校园网建设的重要内容。

基于以上的网络应用需求，新型校园网都会提出建立一个高带宽、高安全、易维护、可扩展以及真正适合应用特点的新型校园网的建设思路，对校园网的方案设计和设备选型做出严格的要求：

（1）校园网必须满足网络应用的特殊要求。校园网项目在设备上需要定制化设计。这主要基于原有的网络设施特点和网络构建成本考虑，涉及机箱尺寸、端口数量、安全性能等方面，这就要求设备供应商应该能够进行定制化设计，提供与网络应用需求吻合的网络设备。

（2）校园网必须具备高带宽及一定的 QoS 保证。由于在目前的校园网络应用中，语音、图形、视频等多媒体数据传输量越来越大，网络首先要为这些数据的稳定传输提供高质量的带宽保证，因此校园网对带宽的需求要远高于同等规模的企业网络。因为在许多高校的校园网中，需要同时传输几十路乃至上百路的视频点播及多媒体课件数据，所以在条件允许的情况下，应尽可能使用链路聚合以及千兆以太网技术构建高带宽网络主干。

（3）校园网络还应该具备较高的性价比，易于应用和维护。与其他行业相比，学校的资金较为有限，校园网对于性能的要求又较高，因此对于性价比的要求自然较高。

（4）网络还必须具备良好的升级扩展能力，同时对安全性和可靠性提供更高的保障。校园网设计必须考虑今后学校业务的发展情况，确保网络设备及网络结构都具有很好的升级扩展能力，同时还要保证升级时能尽可能利用原有设备，以保护投资，实现网络优化。出于可靠性和安全性考虑，应选择一个在网络领域具有规模运营经验的合作厂商。从技术应用角度来看，还应采用冗余备份技术，提高网络稳定性能。在安全设计方面，可以考虑使用划分 VLAN 和安装防火墙，以提高网络安全性。

下面以某学院的网络建设实例来对校园网的建设加以说明。

1．背景

随着信息技术的飞速发展，我国教育行业的信息化建设逐步展开。从技术上看，教育信息化的基本特点是数字化、网络化、智能化和多媒体化，主要基础设施是各学校的校园网和一些区域性的教育信息网络和数据中心。在网络建设过程中，教育单位应该特别注重全面分析自身的网络需求，选择高品质的产品和合适的解决方案，以避免网络不畅、应用脱节、信息“孤岛”、缺少互操作能力、安全防范能力差、管理不便等现象的发生，最大限度地发挥网络在整合教育资源以及办公、管理自动化等方面的作用，为教学、科研、交流、管理等活动提供全面支持。很多国内、外著名的网络设备和解决方案提供商（如 Cisco、D-Link、锐捷公司等）积极致力于中国的信息化建设，针对教育行业的应用趋势和特点，推出全方位、多层次的定制化教育解决方案并得到广泛应用，充分展示出在此领域的整合能力和综合实力。

2．网络需求

某学院的规模为 8000 多人，该学院推行“学做合一、手脑并用”的教育理念，对以校园网为基础的信息化建设十分重视。

该学院占地 60 多公顷，拥有多个网络机房，计算机上千台，多媒体教室几十个以及数量众多的实验室等。计划搭建的校园网需要覆盖包括教学大楼、行政楼、图书馆、实训楼、商业楼、学生宿舍楼以及食堂在内的多栋楼宇，为学院的内部教学和办公管理提供高效的网络环境。网络中的多媒体应用频繁，校园网需要具备良好的稳定性和出色的传输能力。近年来，学院的发展速度很快，因此，方案在设计之初应该把实现网络的弹性扩展作为重要原则，充分考虑到日后的网络升级和软件应用等情况，具备开放性、标准化、先进性等特点，能有效保护学院的投资。该学院与加拿大等国家的院校保持着良好的交流合作关系，校园网需要为对外交流与合作提供便利的网络环境。另外，该学院还需要一套集中的、灵活的管理策略，以便能够轻松实现认证、计费和各类日常管理，有效地集合和调配教学资源。

3．网络结构

在充分考虑该学院的应用需求的基础上，结合已经在教育行业组建过的丰富经验，创新思维，整合致用，采用千兆技术，应用了包括 D-Link 和 Cisco 的产品，实现网络设备的强强联合，进行优化组网，对校园网解决方案进行全盘统筹，还特别采用了先进的网管系统以轻松实现对不同品牌网络设备的全面管理，保证建成的校园网具有电信级的稳定性和可靠性、良好的扩展性以及出色的全网管理能力，为学院进行种类丰富的网络应用提供了坚实的基础。

该学院校园网的拓扑结构如图 10.1 所示。

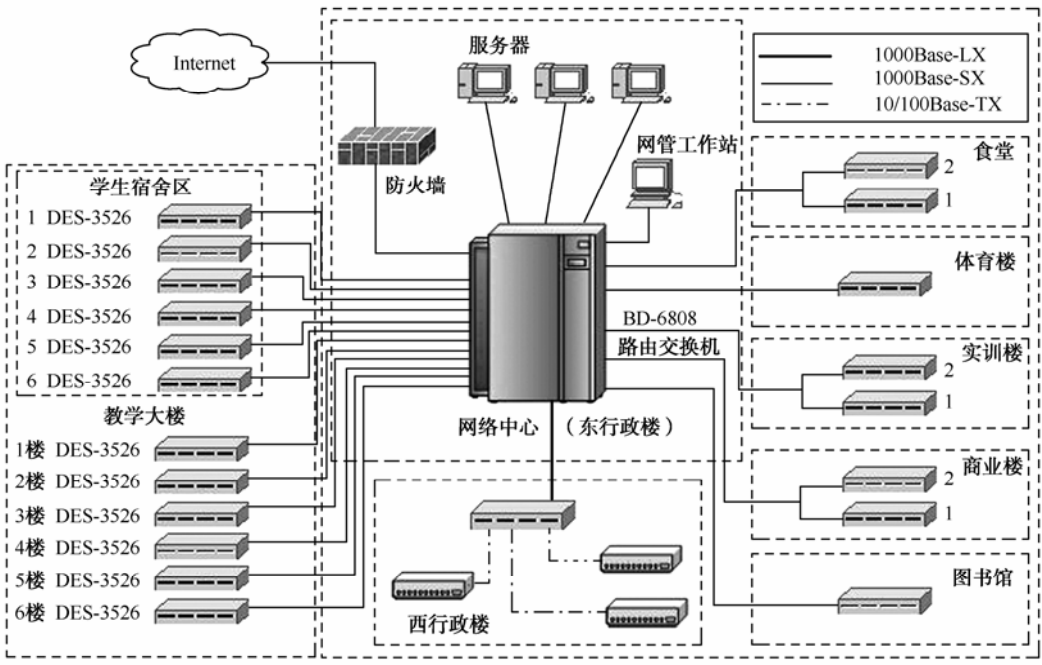


图 10.1　某学院校园网的拓扑结构

该方案将 D-Link 的 Extreme 交换机产品 BD-6808 作为网络中心，安装在学院的东行政楼，分别与防火墙、网管工作站以及服务器群相连接。在教学大楼、图书馆、西行政楼、实训楼、体育楼、商业楼、学生宿舍区以及食堂等建筑中选用高性能的 D-Link 的 DES-3526 二层可堆叠交换机进行接入，西行政楼在 DES-3526 的基础上又进一步部署了多台 DES-1024R＋非网管 10/100Mbps 工作组交换机，东、西行政楼之间用光纤连接（1000Base-LX），最终形成了一套完整有序的网络解决方案。

核心层采用 BD-6808 核心交换机，接入层采用 DES-3526 二层可堆叠交换机，凭借两款产品相得益彰的性能配合，D-Link 的解决方案能够保证校园网具备更出色的千兆表现。BD-6808 交换机采用双引擎，最大千兆端口数可达到 192 个，具有 256Gbps 无阻塞的传输速率，高达 384Gbps 的交换能力，具备冗余和负载均衡特性，通过堆叠主干路由及无阻塞的线速交换满足不断增长的网络系统需求，它与 DES-3526 采用 6 类双绞线连接（1000Base-SX），为学院校园网提供了强劲的千兆核心。

为了保证核心设备的优势得到充分释放，接入层设备需要在诸多性能上与之全面匹配，DES-3526 二层可堆叠交换机凭借灵活的千兆上连、稳定的传输、高效的虚拟堆叠、增强的网

络性能、出色的安全性和管理性等优势成为接入的首选产品。DES-3526 具有 24 个 10/100Base-TX 端口和 2 个组合式 1000Base-T/SFP 端口，可以提供更加安全及灵活的连接方式。在支持多达 32 台设备虚拟堆叠的同时，DES-3526 实现了共用一个 IP 地址管理，兼具大型机柜的扩展性和智能交换机的管理优势。它还支持 IGMP 等组播协议，可以很好地支持视频流，特别适合校园网多媒体应用频繁的情况。

DES-3256 还提供了一套完整的安全保障措施，包含基于 MAC 地址的访问控制列表（ACL）、交换机端口表、IP 地址表、TCP/UDP 端口号、802.1x 网络访问控制协议的用户授权和 MAC 地址控制等措施，不仅能保证用户的正常访问，而且还能阻断恶意的大流量数据在网络中传播，满足了校园网对安全的要求。

校园网对于网络的可靠性和稳定性有着很高的要求，因此，D-Link 在核心层和接入层的设计上进行了全面考虑。核心层采用的 BD-6808 具有出色的冗余能力和负载均衡特性，支持多选径路由，提供基于底板系统的容错能力和可靠性，保证了网络具有足够支持关键任务的能力。接入层的 DES-3526 交换机采用了冗余电源设计，支持 802.3.ad 链路聚合协议、802.1d 生成树协议和 802.1w 快速生成树协议，增加了虚拟堆叠的网络可靠性和可用性。这样的组合有效地保证了可靠性贯穿网络的各个层次，从而提高了网络系统的整体性能。

在网络管理方面，BD-6808 能够提供简洁明了的网络系统拓扑，DES-3526 应用了 D-Link 的最新单一 IP 管理技术，通过结合两者的管理优势大大提高了网络资源的利用率。D-Link 特别在网管工作站安装了自行研发的 D-Vision 网管系统，以便实现对包括 BD-6808、DES-3526 等不同品牌在内的所有网络设备进行监控和管理，使整个校园网的管理一气呵成，成为该方案在管理方面的一大亮点。这套基于 Windows 平台的网管系统具有出色的兼容性，能够轻松实现对网络中所有像 D-Link 品牌网络设备一样具有通用 SNMP 功能的网络设备的全面管理，支持的产品类型十分广泛，大大方便了学院的使用。该系统基于全中文界面进行管理，功能相当完善，实用性很强，能够提供整个网络的拓扑结构和常用网络管理信息，使校园网实现了“垂直＋水平”的管理特性，为校园网带来“专业管理轻松自如”的便利。

西行政楼是学院进行办公、管理的主要场所，D-Link 在这部分设计了基于 DES-1024R＋10/100Mbps 工作组交换机建立的工作组网，为用户提供了百兆快速连接的便利。DES-1024R＋提供 24 个 10/100Mbps 端口，所有端口都支持 Nway 功能、10/100Mbps 自适应及全双工/半双工自动调协，具备流量控制特性，从而保证网络传输更加流畅，网络运行更加稳定、可靠。

4．方案特点

从整体来看，该学院校园网解决方案具有如下特点：

（1）方案所采用的产品全部基于国际标准或者业界标准，具有出色的互操作性，不同设备之间完全能够实现良好的协同工作。从设备的选择来看，D-Link 充分利用了自身的技术优势和行业经验，结合该学院在技术、资源、管理等方面的需求，本着提供高性能网络的原则，将 BD-6808 与 DES-3526 的性能优势全部有效整合到该解决方案中，为学院搭建了高品质、高可靠的校园网，可以说 D-Link 产品的出色性能和兼容性促进了其他厂商产品在该方案中的运用。

（2）该校园网具有良好的可靠性和出色的传输能力。它不仅具备强化的多媒体及 QoS 功能支持，可满足大流量视频、音频的传输需求，还提供了冗余和负载均衡等关键特性，为学院网络的无间断顺畅运行奠定了坚实的基础。

（3）方案为校园网提供了灵活、系统的管理系统。网管系统的应用是一大亮点，凭借其

出色的兼容性和全面的管理能力，结合 DES-3526 的单一 IP 管理技术，对所有支持通用 SNMP 的网络设备都能进行全面的监控和管理。这些管理模块能无缝地集成到网管方案中，使网络管理任务被大大简化，保证了学院对网络资源的充分利用。

（4）该方案为校园网提供了安全的具备高扩展性的网络解决方案。DES-3526 交换机的采用，既使用户获得了 ACL、交换机端口表、IP 地址表、TCP/UDP 端口号、802.1x 和 MAC 地址控制等丰富的安全策略，也使用户能够根据校园网的发展来增加新模块和堆叠交换机数量，实现网络轻松扩展并有效节省了投资。

综观整套方案，充分把握了学院在技术、资源、管理方面的特点，为校园网提供了一套集基础建设、管理方案和扩展方案于一体的完整的解决方案，实现了课件、多媒体等多种教学资源的共享和学校内部即时的沟通，为学院进行对外交流、高效办公提供了便利的环境，大大提升了员工的工作效率和学校的管理质量。该方案所具有的良好的标准性和互操作性也为学院集成丰富的教学、管理等软件应用打开了方便之门，使学校的教学理念和教学方针得到更好的贯彻。此方案的成功实施表现出强大技术实力和全案整合能力，也为学校建设高品质网络提供了重要参考。

本 章 小 结

本章讲述了计算机网络工程的一般概念、并在此基础上对网络需求分析、网络设计的一般原则做了必要介绍，最后通过一个实例说明网络工程设计与实现的过程。

计算机网络工程是在信息工程方法和完善的组织机构的指导下，根据网络应用的需要，按照计算机网络系统的标准、规范和技术、详细规划和设计可行方案，将计算机网络硬件和设备、软件和技术系统性地集成在一起，成为满足用户需求、高性价比的计算机网络系统的组建过程。

需求调查的关键是与客户的沟通，要使客户满意。

需求分析找出“需”和“求”的关系，从当前业务中找出最需要重视的方面，从已经运行的网络中找出最需要改进的地方，满足客户提出的各种合理要求，依据客户要求修改已经成形的方案。

在系统建设中，网络系统建设将遵循先进性、实用性、可扩充、可维护性、可靠性、经济性等原则进行系统的规划、分析、设计、开发、维护和项目的管理。

思 考 题

1．如何做企业网络设计的需求分析？
2．网络设计的一般建设原则有哪些？
3．如何根据企业网络的具体需求，做一个计算机网络解决方案？

实训 16　校园网的方案设计

一、实训目的

1．理解网络设计和规划的方法及意义。

2．熟悉设计的工具，如 Visio 等。

3．进一步了解网络硬件的组成及各部分之间的关系。

二、实训环境

1．局域网环境。

2．装有 Visio 等软件的 PC。

三、实训内容

现有一所大学，情况如下：

该学校的主校区有教学楼和实验楼共 6 座，每座有 8～9 层，每层有 6 间教室和 2 间教师备课室。

该学校的外校区有教学楼和实验楼共 4 座，每座有 5 层，每层有 5 间教室和 2 间教师备课室。

每间课室暂时提供 2 台计算机，教师办公室提供 3～5 台计算机，另有 8 个 60 台机器的计算机实验室。

每个校区各有学生宿舍 4 座，每座有 7 层，每层有 8 间房，每间房有 6 个学生，拟保证每个学生有一个上网端口。

在教育网申请 16 个正式 C 类 IP 地址，IP 地址为 202.188.1/20。

现请你规划校园网 IP 地址，要求如下：

每校区在网管中心设置 1 台主机（提供对外个人主页服务）、1 台邮件服务/FTP 服务器、2 台校内服务器。在主校区设置总服务器 1 台。学生机器采用私有 IP 地址，通过代理服务器上校外网。教师采用正式 IP 直接上校外网，并能浏览校内服务器。设计时，应尽量能够减少广播风暴，有一定的扩充余地，每个校区采用的私有 IP 应尽量集中，方便网管人员统一管理，要求有较高的安全性。

四、实训报告要求

根据以上环境和设计要求，写出各服务器的 IP 地址配置和私有 IP 地址的分配方案，并写出相应的简要理由。

第 11 章　计算机网络技术的新发展

本章要点

本章从多层交换概念入手，首先介绍第三层、第四层、第七层交换技术，然后探讨 IPv6 技术，最后简要介绍网格技术、P2P。

本章目标

- 了解多层交换的概念
- 了解 IPv6 的产生
- 掌握 IPv6 的地址表示方法
- 了解 IPv4 到 IPv6 的过渡方法
- 了解网络技术的应用
- 了解 P2P 技术及应用

网络技术是一个优胜劣汰的发展过程。以 Internet 为代表的新技术革命正在深刻地改变着传统的网络观念和体系结构。多层交换技术的出现，解决了局域网中网段划分之后，网段中的子网必须依赖路由器进行管理的局面，解决了传统路由器低速、复杂所造成的网络瓶颈问题。IPv6 使网络摆脱了地址和空间的限制，成为三网（电话网、计算机网、有线电视网）融合的黏合剂。统一的 IP 协议的普遍采用，使得各种以 IP 为基础的业务都能在不同的网络上实现互通。网格计算是互联网发展的前沿领域，其本质是全球万维网升级至全球大网格。P2P 技术的飞速发展，使互联网的存储模式由目前的“内容位于中心”模式转变为“内容分散存储”模式。

11.1　多层交换技术

多层交换是相对于传统交换的概念而提出的。众所周知，传统交换技术是在 OSI 网络模型中的第二层（数据链路层）中进行操作的，而多层交换技术是在网络模型中的第三层以上实现了数据包的高速转发。多层交换技术并不是网络交换机与路由器的简单堆叠，而是二者的有机结合，形成一个集成的、完整的解决方案。

11.1.1　第三层交换

1．什么是三层交换

三层交换技术也称为 IP 交换技术、高速路由技术等。这是一种利用第三层协议中的信息来加强第二层交换功能的机制。当今，绝大部分的企业网都已变成实施 TCP/IP 的 Web 技术的内联网，用户数据往往越过本地网络在网际间传送，因而路由器常常不堪重负。一种办法是安装性能更强的超级路由器，然而，这样做的开销太大，如果是建交换网，这种投资显然

是不合理的。第三层交换的目标是，只要在源地址和目的地址之间有一条更为直接的第二层通路，就没有必要经过路由器转发数据包。第三层交换使用第三层路由协议确定传送路径，此路径可以只用一次，也可以存储起来，供以后使用。之后，数据包通过一条虚电路绕过路由器快速发送。

2．第三层交换技术

目前，主要有下列第三层交换技术。

（1）Ipsilon IP 交换：IP 交换技术由 Ipsilon 公司首倡，即识别数据包流，尽量在第二层进行交换，以绕过路由器，改善网络性能。该技术适用于机构内部的局域网和校园网。

（2）Cisco 标签交换：给数据包贴上标签，此标签在交换节点读出，判断包传送路径。该技术适用于大型网络和 Internet。

（3）3Com Fast IP：侧重数据策略管理、优先原则和服务质量。Fast IP 保证实时音频或视频数据流能得到所需的带宽。Fast IP 支持其他协议（如 IPX），可以运行在除 ATM 外的其他交换环境中。客户机需要有设置优先等级的软件。

（4）IBM ARIS（Aggregate Route-Based IP Switching）：与 Cisco 的标签交换技术相似，包上附上标记，借以穿越交换网。ARIS 一般用于 ATM 网，也可扩展到其他交换技术。边界设备是进入 ATM 交换环境的入口，含有第三层路由映射到第二层虚电路的路由表。允许 ATM 网同一端两台以上的计算机通过一条虚电路发送数据，从而减少网络流量。

（5）MPOA（MultiProtocol Over ATM）：ATM 论坛提出的一种规范。经源客户机请求，路由服务器执行路由计算后给出最佳传输路径。然后，建立一条交换虚电路，即可越过子网边界，不用再做路由选择。

3．第三层交换技术的演变

下面以 3Com 公司的技术为例，来说明第三层交换技术的演变。

第一代交换机是分立的电子元件和原语式的软件框架的混合体。软件的功能运行在一个有固定内存的处理机上，随着管理支持和协议功能的改善，软件的功能也不断增加。当用户的日常业务更加依赖于网络、网络上的流量增多时，网络设备便成了瓶颈。

虽然处理机和存储器变得越来越快和有效，但仍然赶不上流量增加的水平。解决问题的第一步是简化网络层：用交换机取代路由器，以减低处理数据包的开销并显著地提高事务处理速度。3Com 引进了专用于优化第二层处理的专用集成电路（ASIC），使性能提高了 10 倍，并降低了系统的整体费用。

灵活智能的路由引擎（FIRE）宣告了第三代交换技术的来临。这一代并不仅是建立在第二代的进展上，而且为第三层路由、组播（Multicast）及用户可选的策略（Policy）等方面提供了线速性能，第二层与第三层的性能不再是不一致的了。

FIRE 是 3Com 公司的第三代第三层交换机的核心部分，它是一个创新的集成化的网间互联体系结构，提供了广泛的第二层和第三层的功能，同时还可在多种网络接口类型上提供线速性能。

11.1.2　第四层交换

端到端性能和服务质量要求对所有连网设备的负载进行细致的均衡，以保证客户机与服务器之间的数据平滑地流动。 第二层与第三层交换产品在解决局域网和互联网络的带宽及容量问题上发挥了很好的作用，但是，这可能还不够，还需要更多的性能，而这正是第四层交

换的用武之地。

第四层交换技术利用第三层和第四层包头中的信息来识别应用数据流会话，这些信息包括 TCP/User 数据报协议（UDP）端口号、标记应用会话开始与结束的“SYN/FIN”位以及 IP 源/目的地址。利用这些信息，第四层交换机可以做出向何处转发会话传输流的智能决定。对于使用多种不同系统来支持一种应用的大型企业数据中心、Internet 服务提供商或内容提供商来说，第四层交换的作用是尤其重要的。同样，在很多服务器上进行复制功能时，第四层交换也会起到不小的作用。

路由器和第三层交换机在转发不同数据包时并不了解哪个包在前哪个包在后。第四层交换技术从头至尾跟踪和维持各个会话。因此，第四层交换机是真正的“会话交换机”。

11.1.3 第七层交换

目前，特别是在高可用性和负载均衡方面，有许多先进的工具可以利用由应用返回给最终用户的第七层信息。这类工具使用户可以容易地确认站点内容的响应性和正确性，或从用户的角度来试测你的站点，看看是否存在正确的应用和内容。

用户不仅能验证是否在发送正确的内容，而且还能打开网络上传送的数据包（不用考虑 IP 地址或端口），并根据包中的信息做出负载均衡决定。

从本质上讲，这种智能性迁移超越了第四层的功能。以端口 80 为例，除了一般类型的 Web 传输流之外，还有许多类型的传输流流过此端口。最多具有第四层功能的设备无法识别流过此端口的不同类型的传输流，因此它们同等对待所有传输流。

但是，传输流并不都是相同的。对于负载均衡产品来说，能够知道流过此端口的数据是流媒体还是对商品目录中一件商品的简单请求非常有用，也许商家想赋予需要此目录项的客户更高的优先级。不少具有第四层功能的设备以同样的方式对待这两种类型的数据，因而可能将流媒体数据发送到无法做出响应的服务器，导致错误的信息和时延。

第七层的智能性能够进行进一步的控制，即对所有传输流和内容的控制。由于可以自由地完全打开传输流的应用/表示层，仔细分析其中的内容，因此可以根据应用的类型而非仅根据 IP 和端口号做出更智能的负载均衡决定。

这就可以不仅仅基于 URL 做出全面的负载均衡决策，而且还能根据实际的应用类型做出决策，无论这些应用正使用什么端口号。这将使用户可以识别视频会议流，并根据这一信息做出相应的负载均衡决策，尽管该应用可能正在使用动态分配地址。

这类具有第七层认知的产品的部分功能是保证不同类型的传输流可以被赋予不同的优先级。具有第七层认知的设备不是依赖路由设备或应用来识别差别服务（Diff-Serv）、通用开放策略服务或其他服务质量协议的传输流，它可以对传输流进行过滤并分配优先级。这就使用户不必依赖应用或网络设备来达到这些目的。

目前，还没有第七层功能的标准。具有第七层认知的功能具有很大的互补性，它可以与提供 Diff-Serv 这类服务的网络和谐共存。它对传输流进行分析，然后判定，如对于 IP 语音这个传输流就需要设置服务比特位，而对于其他类型的传输流只需要设置较低优先级类型的服务比特位。

过去，用户总需要在智能性与速度之间进行权衡。在采用第七层认知技术的情况下，可以以线速度做出更智能性的传输流决策。用户将自由地根据得到的信息就各类传输流和其目的地做出决策，从而优化 Web 访问，为最终用户提供更好的服务。

综上所述，第七层交换可以实现有效的数据流优化和智能负载均衡。

11.2 下一代互联网协议 —— IPv6

11.2.1 IPv6 概述

IPv6 是“互联网协议第 6 版”的缩写。IPv6 是由 IETF 设计的下一代互联网协议，目的是取代现有的互联网协议第 4 版（IPv4）。随着新应用的不断涌现，传统的 IPv4 协议已经难以支持互联网的进一步扩张和新业务的特性，其不足主要体现在以下方面。

（1）地址资源即将枯竭：IPv4 提供的 IP 地址位数是 32 位，即约 1 亿个地址。随着连接到 Internet 上的主机数目的迅速增加，有预测表明，所有 IPv4 地址将在 2005—2010 年间分配完毕。

（2）路由表越来越大：由于 IPv4 采用与网络拓扑结构无关的形式来分配地址，所以随着连入网络数目的增加，路由器数目飞速增加，相应地，决定数据传输路由的路由表也就不断增大。

（3）缺乏服务质量保证：IPv4 遵循 Best Effort 原则，这一方面是一个优点，因为它使 IPv4 简单高效；但另一方面它对互联网上涌现出的新业务类型缺乏有效的支持，如实时和多媒体应用要求提供一定的服务质量保证，如带宽、延迟和抖动等。

（4）地址分配不便：IPv4 采用手工配置的方法给用户分配地址，这不仅增加了管理和规划的复杂程度，而且不利于为那些需要 IP 移动性的用户提供更好的服务。

IPv6 能够解决 IPv4 的许多问题，如地址短缺、服务质量保证等。同时，IPv6 还对 IPv4 做了大量的改进，包括路由和网络自动配置等。IPv6 和 IPv4 将在过渡期内共存几年，并由 IPv6 渐渐取代 IPv4。相对于 IPv4，IPv6 有如下一些显著的优势。

（1）地址容量大大扩展，由原来的 32 位扩充到 128 位，彻底解决 IPv4 地址不足的问题；支持分层地址结构，从而更易于寻址；扩展支持组播和任意播地址，使数据包可以发送给任何一个或一组节点。

（2）大容量的地址空间能够真正地实现无状态地址自动配置，使 IPv6 终端能够快速连接到网络上，无需人工配置，实现了真正的即插即用。

（3）报头格式大大简化，从而有效减少路由器或交换机对报头的处理开销，这对设计硬件报头处理的路由器或交换机十分有利。

（4）加强了对扩展报头和选项部分的支持，这除了让转发更为有效外，还为将来网络加载新的应用提供了充分的支持。

（5）流标签的使用可以为数据包所属类型提供个性化的网络服务，并有效保障相关业务的服务质量。

（6）认证与私密性：IPv6 把 IPSec 作为必备协议，保证了网络层端到端通信的完整性和机密性。

（7）IPv6 在移动网络和实时通信方面有很多改进。特别是，与 IPv4 相比，IPv6 具备强大的自动配置能力，从而简化了移动主机和局域网的系统管理。

11.2.2 IPv6 报头的结构

新的 IPv6 报头的结构比 IPv4 简单得多，IPv6 报头中删除了 IPv4 报头中许多不常用的域，放入了可选项和报头扩展中；IPv6 中的可选项有更严格的定义。IPv4 中有 10 个固定长度的域、2 个地址空间和若干个选项，IPv6 中只有 6 个域和 2 个地址空间。

虽然 IPv6 报头占 40 字节，是 24 字节 IPv4 报头的 1.6 倍，但因其长度固定（IPv4 报头是变长的），故不需要消耗过多的内存容量。

IPv4 中的报头长度（Header Length）、服务类型（Type of Service，TOS）、标志符（Identification）、标志（Flag）、分段偏移（Fragment Offset）和报头校验和（Header Checksum）这 6 个域被删除。报文总长（Total Length）、协议类型（Protocol Type）和生存时间（Time to Live，TTL）3 个域的名称或部分功能被改变，其选项（Options）功能完全被改变，新增加了 2 个域，即优先级和流标签。

IPv4 与 IPv6 报头的比较如图 11.1 所示。

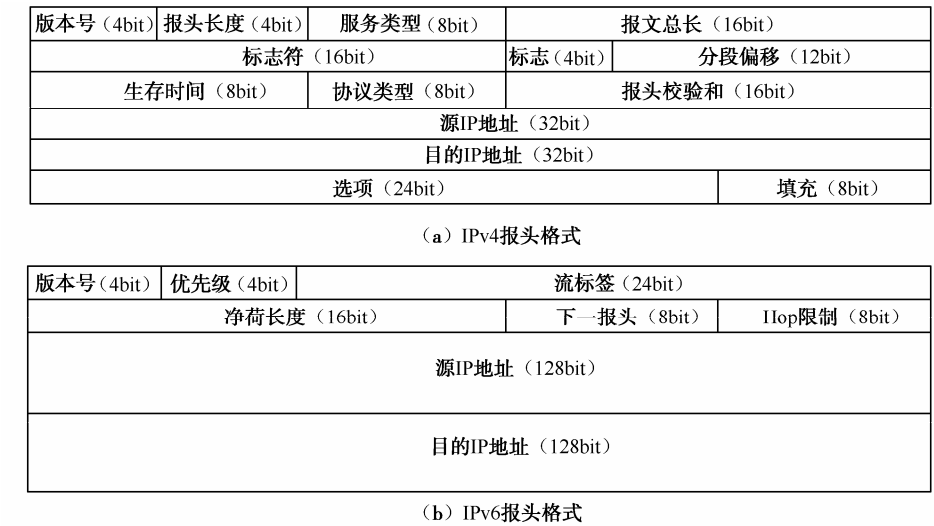


图 11.1　IPv4 与 IPv6 报头的比较

11.2.3 IPv6 地址

IPv4 地址表示为点分十进制格式，32 位的地址分成 4 个 8 位分组，每个 8 位写成十进制数，中间用点号分隔。IPv6 的 128 位地址以 16 位为一分组，每个 16 位分组写成 4 个十六进制数，中间用冒号分隔，称为冒号分十六进制格式。

例如，21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A 是一个完整的 IPv6 地址。

IPv6 的地址表示有以下几种特殊情形。

（1）在 IPv6 地址中，每个 16 位分组中的前导零位可以去除做简化表示，但每个分组必须至少保留 1 位数字。如上例中的地址，去除前导零位后可写成：21DA:D3:0:2F3B:2AA:FF:FE28:9C5A。

（2）某些地址中，可能包含很长的零序列，为进一步简化表示法，还可以将冒号十六进制格式中相邻的连续零位合并，用双冒号“::”表示。“::”符号在一个地址中只能出现一次，该符号也能用来压缩地址中前部和尾部的相邻的连续零位。例如，地址 1080:0:0:0:8:800:200C:417A，

0:0:0:0:0:0:0:1，0:0:0:0:0:0:0:0 分别可表示为压缩格式 1080::8:800:200C:417A，::1，:: 。

（3）在 IPv4 和 IPv6 混合环境中，有时更适合于采用另一种表示形式：x:x:x:x:x:x:d.d.d.d，其中 x 是地址中 6 个高阶 16 位分组的十六进制值，d 是地址中 4 个低阶 8 位分组的十进制数（标准 IPv4 表示）。例如，地址 0:0:0:0:0:0:13.1.68.3，0:0:0:0:0:FFFF:129.144.52.38 写成压缩形式为::13.1.68.3，::FFFF.129.144.52.38。

（4）要在一个 URL 中使用文本 IPv6 地址，文本地址应该用符号“[”和“]”来封闭。例如文本 IPv6 地址 FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 写做 URL 示例为 http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html。

11.2.4 IPv4 到IPv6 的过渡

如何完成从 IPv4 到 IPv6 的转换，是 IPv6 发展中需要解决的第一个问题。目前，IETF 已经成立了专门的工作组，研究 IPv4 到 IPv6 的转换问题，并且提出了很多方案，主要包括以下 4 个类型。

1．隧道技术

随着 IPv6 网络的发展，出现了许多局部的 IPv6 网络，利用隧道技术可以通过现有的运行 IPv4 协议的 Internet 骨干网络（即隧道）将局部的 IPv6 网络连接起来，因而是 IPv4 向 IPv6 过渡的初期最易于采用的技术。隧道技术的方式为：路由器将 IPv6 的数据分组封装入 IPv4，IPv4 分组的源地址和目的地址分别是隧道入口和出口的 IPv4 地址。在隧道的出口处，再将 IPv6 分组取出转发给目的站点。

2．网络地址转换/协议转换技术

网络地址转换/协议转换技术（Network Address Translation-Protocol Translation，NAT-PT）通过与 SIIT 协议转换、传统的 IPv4 下的网络地址翻译（NAT）以及适当的应用层网关（ALG）相结合，实现了只安装了 IPv6 的主机和只安装了 IPv4 机器的大部分应用的相互通信。

3．IPv6/IPv4 双协议栈技术

简单地说，双栈机制就是使 IPv6 网络节点具有一个 IPv4 栈和一个 IPv6 栈，同时支持 IPv4 和 IPv6 协议。IPv6 和 IPv4 是功能相近的网络层协议，两者都应用于相同的物理平台，并承载相同的传输层协议 TCP 或 UDP。如果一台主机同时支持 IPv6 和 IPv4 协议，那么该主机就可以与仅支持 IPv4 或 IPv6 协议的主机通信。IPv6/IPv4 双协议栈的协议结构如图 11.2 所示。

图 11.2　IPv6/IPv4 双协议栈的协议结构

4．应用服务系统（DNS）过渡技术

在 IPv4 到 IPv6 的过渡过程中，作为 Internet 基础架构的 DNS 服务也要支持这种网络协议的升级和转换。IPv4 和 IPv6 的 DNS 记录格式等方面有所不同，为了实现 IPv4 网络和 IPv6 网络之间的 DNS 查询和响应，可以采用应用层网关 DNS-ALG 结合 NAT-PT 的方法，在 IPv4 和 IPv6 网络之间起到一个翻译的作用。例如，IPv4 的地址域名映射使用“A”记录，而 IPv6 使用“AAAA”或“A6”记录。那么，IPv4 的节点发送到 IPv6 网络的 DNS 查询请求是“A”

记录，DNS-ALG 就把“A”改写成“AAAA”，并发送给 IPv6 网络中的 DNS 服务器。当服务器的回答到达 DNS-ALG 时，DNS-ALG 修改回答，把“AAAA”改为“A”，把 IPv6 地址改成 DNS-ALG 地址池中的 IPv4 转换地址，把这个 IPv4 转换地址和 IPv6 地址之间的映射关系通知 NAT-PT，并把这个 IPv4 转换地址作为解析结果返回 IPv4 主机。IPv4 主机就以这个 IPv4 转换地址作为目的地址与实际的 IPv6 主机通过 NAT-PT 通信。

上述技术在很大程度上依赖于从支持 IPv4 的互联网到支持 IPv6 的互联网的转换，期待 IPv4 和 IPv6 可在这一转换过程中互相兼容。目前，6 to 4 机制是较为流行的实现手段之一。

11.2.5 几种IPv6 应用介绍

从语音、数据到视频，从对现有网络应用更卓越的支持与改善，到 IPv6 独具特色的创新业务，IPv6 带给我们的全方位、高品质的应用与服务前景是美妙而广阔的。以下简单介绍几种 IPv6 应用。

1．视频应用

IPv6 对于视频应用的意义是：解决了地址容量问题；优化了地址结构，以提高选路效率；提高了数据吞吐量，以适应视频通信大信息量传输的需要。IPv6 还加强了组播功能，实现了基于组播、具有网络性能保障的 VC 视频会议、高清晰度数字电视、VOD 视频点播、网络视频监控应用。这是只有高带宽、高性能的下一代互联网才能支持的典型应用，具有交互协同技术特性。IPv6 对 IPv4 的最大革新是对于 QoS 的考虑，对各种多媒体信息根据紧急性和服务类别确定数据包的优先级。此外，IPv6 采用必选的 IPSec 很好地保证了网络的安全性。

2．移动智能终端应用

传统的移动通信技术主要是为了支撑话音业务，虽然随着用户需求的提出和技术的发展，目前已经有了基于 WAP 或 GPRS 提供 IP 业务的蜂窝电话产品，但是现有的技术远远无法满足未来通信的需要，第三代移动通信将采用分组交换的设备来代替电路交换设备，IP 业务将是第三代移动通信业务中的重要组成部分。

由于 IP 的诸多优点和全球 IP 浪潮的影响，3G 演变为全 IP 的趋势越来越明显。作为移动通信的核心，3G 为了满足始终在线的需求，需要很大的地址空间，只有 IPv6 才能满足这种需求。

3G 的发展方向将是一个全 IP 的分组网络，3G 业务将以数据和互联网业务为主，在 3G 网络上将承载着实时话音、移动多媒体、移动电子商务等多种业务，因此在计费、漫游、应用、终端等方面会更加复杂，IPv6 将是实现这些服务的关键。如果说 3G 的发展推动了 IPv6 的发展和标准化，那么 IPv6 协议的诸多优越特性则为 3G 网络的发展奠定了坚实的基础，IPv6 有庞大的地址空间，对移动性有良好的支持，有服务质量的保证机制、安全性和地址自动分配机制等。3GPP 将 IPv6 作为 3G 必须遵循的标准。国内、外的很多通信厂商正致力于构建基于 IPv6 的全 IP 的 3G 核心网（All-IP Core）。

3．无线网络应用

最近，无线网络 WLAN 在中国的热点地区渐成亮点，随着网络技术和业务的发展，人们将会提出多种接入方式无缝互连的要求，即忽略蓝牙、无线局域网和广域网（GSM/CDMA）之间的技术差异，使得在不同网络环境下用户的连接和所使用的业务不会中断，真正实现不间断的连接。采用移动 IPv6 将使这一目标的实现更加容易。

实现用户通信的同一性：目前一个人拥有多个不同类型的终端（如手机、PDA、笔记本

电脑等）的现象已不鲜见，这些终端普遍都有上网功能，但这些终端的上网是互不相干的，通信的内容、方式也因终端而异。然而，从用户的角度来看，实现通信的同一性是至关重要的，未来的用户应该只关注自己的应用而将终端淡化成一种手段，而以 IPv6 大量的地址资源和其他先进的性能作为基础，完全可以实现用户通信的同一性。

实现多种接入方式的无缝互联：未来各种接入网技术仍然共存，如在 PAN 中采用蓝牙技术、在 LAN 中采用无线局域网（802.11）技术、在 WAN 中采用 WCDMA/GSM 技术等，而无线技术最终将使人们忽略接入技术的不同而实现随时随地的网络连接，用户能够使用一种多模的终端来通过全球移动网络以及有限范围的WLAN或蓝牙系统来接入IP网络或Internet，用户从某种接入技术覆盖的区域移动到另一种接入技术覆盖的区域时，仍然能够保持不间断的连接。

业界的一种观点认为，未来的网络将是全 IP 网络，全 IP 能无缝集成各种接入方式，将宽带、移动 Internet 和现有的无线系统都集成到 IP 层中，通过一种网络基础设施提供所有通信服务，并为运营商带来许多好处，如节省成本、增强网络的可扩展性和灵活性、提高网络运作效率、创造新的收入机会等。采用移动 IPv6 是实现全 IP 网络的最基本的要求。

在电信网方面，越来越多的人认为未来的电信网络是基于 IP 技术的网络。IP 电信网和传统的电信网络存在很大的不同，其力图将自由的 IP 网络变成有序的、可管理的、有 QoS 保障的、以提供增值业务为主的网络。在组建 IP 电信网时，IPv6 是首选的技术之一。

除此之外，在线游戏，网络家电，智能终端的不断发展也会是 IPv6 应用的一个有力的推动因素。总之，要提供 whoever、whenever、wherever 始终在线的服务，只有 IPv6 才能满足要求。

随着我国大规模 IPv6 网络部署的全面展开，IPv6 关键技术研究、重大应用示范以及应用推广于 2004—2005 年陆续启动并全面铺开。中国将在全球 IPv6 的部署进程中发挥越来越重要的作用。我们完全有理由相信，IPv6 产业界的支持者、推动者们将会分享到更多、更新的 IPv6 网络部署以及应用探索的实践成果、经验。

11.3 网格技术

11.3.1 网格简介

网格一词译自英文单词“Grid”，是把整个 Internet 整合成一台巨大的超级计算机，实现计算资源、存储资源、数据资源、信息资源、知识资源、专家资源的全面共享，其规模可以大到某个洲，小到企事业内部、局域网、家庭和个人。

网格所关注的问题无论从范围、程度还是本质上都已经与互联网所关心的互连问题有了很大的不同。Internet 技术和 Web 技术的主要成就是实现了计算机和网页的连通，提供收发邮件、浏览和下载网页信息等相关服务，它所关注的问题是如何使信息传输流量更大、传输速度更快、传输更加安全。网格技术则关注如何有效、安全地管理和共享连接到 Internet 上的各种资源，并提供相应的服务。网格在连通计算机和网页的基础上，还将各种信息资源（如数据库、软件以及各种信息获取设备）都连接成一个整体，整个网络如同一台巨大无比的计算机，向每个用户提供包括计算能力、数据存储能力以及各种应用工具等一体化的透明服务。它强调的是全面地共享资源、全面地应用服务。因为目前的技术还没有实现资源层面的全面

共享，只是信息的传输，所以仍是网络技术，而非网格技术。互联网的新一次浪潮的实质，就是要将万维网（World Wide Web）升华为大型全球网格（Great Global Grid，3G），即实现 WWW 到 GGG 的变革。

网格是借鉴电力网的概念提出的，网格的最终目的是，希望用户在使用网格计算能力解决问题时像使用电力一样方便，用户不用考虑得到的服务来自于哪个地理位置，由什么样的计算设施提供。也就是说，网格给最终使用者提供的是一种通用的计算能力。

在电力网中，需要有大量的变电站等设施对电网进行调控，在网格中也需要有大量的管理站点来维护网格的正常运行。网格的结构及资源的调控更复杂，需要解决的问题也更多。因为网格所关心的问题不再是文件交换，而是直接访问计算机、软件、数据和其他资源，所以要求网格具备解决资源与任务的分配和调度、安全传输与通信实时性保障、人与系统以及人与人之间的交互等能力。网格提供的资源是随时间动态变化的，原来拥有的资源或者功能，在下一时刻可能就会出现故障或者拒绝被使用，而原来没有的资源，可能随着时间的进展会不断加入进来。

目前，在复杂科学计算领域中仍然以超级计算机作为主宰，但是由于其造价极高，通常只用于航天局、气象局这样的国家级部门。网格计算（Grid Computing）作为一种新的计算模式，其低廉的造价和超强的数据处理能力备受青睐。网格作为一个集成的计算与资源环境，能够吸收各种计算资源，将它们转化成一种随处可得的、可靠的、标准的且相对经济的计算能力，其吸收的计算资源包括各种类型的计算机、网络通信能力、数据资料、仪器设备甚至有操作能力的人等各种相关资源。

11.3.2 网格技术的应用

事实上，网格技术的应用离我们的生活并不遥远，在科学研究、企业信息处理、电子政务以及个人娱乐等社会生活的各个领域中都活跃着网格技术的身影。

1．科学研究

现在，科学研究的问题空前复杂化，而科学研究所需要的运算资源常常是捉襟见肘。复杂科学领域的计算通常以超级计算机作为数据处理中心，超级计算机虽然处理能力强大，但是其本身的造价极其高昂，并不是所有的研究机构都有能力配备。网格技术的出现，最大程度地提高了现有网络计算资源的利用率。目前，利用网格提高现有资源利用率主要有以下两种办法。

（1）利用网格技术可以将各个实验室的超级计算机连接起来，形成一个“强强联合”的超级信息处理中心。例如，美国国家科学基金会建立的“分布式太级网格（Tera Grid）”，利用网格技术将伊利诺伊州立大学超级计算中心、圣迭戈大学超级计算中心、阿尔贡国家试验室和加利福尼亚州理工学院计算中心连接起来，形成一个处理能力约为 13.5 万亿次浮点操作每秒，存储容量接近 700TB 的“巨无霸”计算中心，以供许多领域的研究机构使用。

（2）通过互联网，利用互联网个人用户的闲置计算机，进行科学研究。这种方式最为著名的项目就是寻找外星生命的计划 seti@home。1999 年，美国行星学会发表一项公告，呼吁互联网上的天文爱好者参与寻找地球外文明的科学实验。该实验将阿雷西博射电天文望远镜所拍摄到的外太空数据分成若干“小片”，参与该项目的天文爱好者通过下载载有“数据小片”的客户端，该客户端以屏幕保护程序的形式出现，只要计算机处于闲置状态，屏幕保护程序就开始工作，利用本地运算资源分析该“数据小片”，分析完后再将分析结果传回 seti@home

小组。从 1999 年至今，已经有 500 多万台个人计算机在闲置之余参与这项工作，这些利用零星时间所累计起来的计算总量想当于 20 台价值千万美元的超级计算机昼夜不息工作所能达到的计算极限。

2．企业信息处理

IBM 推出一个新的计划，该计划帮助软件厂商开发新的应用程序，并测试现有的应用程序，IBM 为这些软件厂商提供 IBM 网格运算服务器的免费存取权。拥有免费存取权的软件开发人员可以利用 IBM 网格服务器的强大运算资源，快速完成新开发的软件所必需的调试及模拟运算，从而缩短程序从开发到应用的周期，提高软件的开发速度。

当然，这只是网格计算给出的一个例子。实际上，网格所能做的比我们想象的还要多。网格专家为我们描绘的是这样的一幅画面：等网格的触角深及互联网的每一个角落时，从互联网获得网格的运算资源就会像从电网上获取电力那么简单，我们只需要支付少量费用，就可以租用这台“超级信息处理中心”为我们工作。这对于信息处理需求大的企业来讲，无疑是个福音。现在，很多企业为了保证其业务不间断地运转，大多部署了价格不菲的大型 IT 系统，这些 IT 设备除了在少数的业务高峰时间可以得到充分利用外，大部分时间都是闲置的，这些闲置资源无疑导致了企业运行成本的增加。一个强大的可租用虚拟系统，可以让用户完成以前难以承担的任务，其生产成本却不会有明显的增长。

3．电子政务

一提到电子政务，很多人马上就会想到我们的政府网站，想起网站上的政府公告、红头文件。其实，电子政务不仅仅是利用互联网来宣传政府的计划和服务，也不应该只停留在政府文件的“网页化”——利用互联网传达信息只是电子政务的初级阶段，利用互联网进行日常性的政府办公才是真正意义上的电子政务。

网格技术可以整合和管理分散在各部门的信息化资源，实现各个政府部门之间的数据无缝交换，消除“信息孤岛”，打破电子政务资源共享的瓶颈；另外，网格技术的分布式工作模式，可以有效地实现在网络虚拟环境下的协同办公，提高政府的工作效率、增强为公众服务的能力。

正是因为看中了网格技术在电子政务建设方面的优势，上海市政府于 2003 年 7 月与 IBM 中国公司签署了网格计算合作谅解备忘录，旨在利用网格技术解决上海信息港建设中出现的问题（如部门之间的信息化资源分散、跨部门协作缺乏标准、部门间资源共享与协作困难），通过资源的整合，提高信息化建设的整体成效，开创了国内利用网格计算技术推动电子政务发展的先例。相信随着网格技术的进一步发展，网格在电子政务方面的应用会越来越广泛。

4．个人娱乐

随着互联网的发展，网络视频点播与在线游戏已经成为个人娱乐的重要一环。使用网格可以为游戏开发商和服务供应商提供可扩展的、高弹性的基础设施以运行大型多人游戏。美国游戏基础设施提供商 Butterfly.net 公司目前使用的就是 IBM 的网格计算服务器。该服务器利用了网格技术自恢复特性，能够无缝隙地将所玩的游戏转到最近的可用服务器上，实现了用户资源的统一调动、统一保存，极大提高了游戏运行和服务的可扩充性。据 Butterfly.net 与 IBM 的评估，在相同的预定收益中，利用网格技术布置的网格服务器产生的利润是传统集中式服务器的 8 倍。对于个人用户来说，网格服务器意味着更安全、更快捷的游戏体验。

网格技术有望使虚拟现实技术走向平民化。虚拟现实（Virtual Reality）技术是一种利用计算机图形技术人工合成的可以按照用户的输入而变化的模拟仿真环境、一个多维信息空间、

一个用户可与计算机系统自然交互的三维人机界面。虚拟现实技术的最大优点是，可以通过各种传感器获得虚拟环境给予的各种体验。由于运行虚拟现实技术所需要的计算资源过于庞大，所以虚拟现实技术目前只用于飞行员、宇航员等的训练工作，普通个人根本无法享受这一技术带来的娱乐体验。利用网格这种造价低廉而数据处理能力超强的计算模式，可以将虚拟现实技术运用于网络游戏中，让参与游戏的人可以真切地感受虚拟环境所带来的游戏快感。毫无疑问，如果这一技术移植成功，将使目前的网络游戏发生革命性变化。

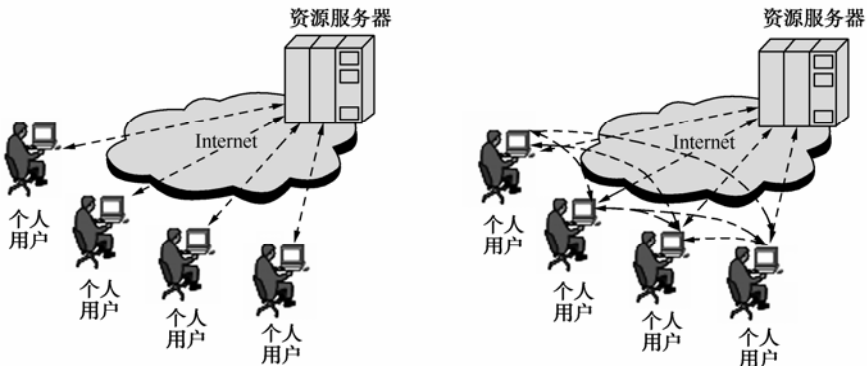
当然，在网格技术走向大规模应用时，也存在着不少问题，如各个公司之间的技术标准不统一、并非所有的软件都支持分布式计算、分享服务器会带来数据安全问题；还有些非技术性问题，如人们对新技术成熟与否、共享资源是否导致丧失对资源控制权的担忧，也成为网格技术进一步普及的障碍。

11.4 P2P网络

11.4.1 P2P简介

P2P 是“Peer-to-Peer”的缩写，称为对等网。P2P 是一种分布式网络，其中的参与者共享他们所拥有的一部分硬件资源，这些共享资源需要由网络提供服务和内容，能被其他 Peer 直接访问而无需经过中间实体。在此网络中的参与者既是资源提供者，又是资源获取者。P2P 起源于最初的连网通信方式，如在建筑物内，PC 通过局域网互连，不同建筑物间通过 MODEM 远程拨号互连。其中建立在 TCP/IP 之上的通信模式构成了今日互联网的基础，因此，从基础技术角度看，P2P 不是新技术，而是新的应用技术模式。

由于 P2P 技术的飞速发展，互联网的存储模式将由目前的“内容位于中心”模式转变为“内容分散存储”模式。传统的 Internet 流量模型和 P2P 流量模型的区别如图 11.3 所示。



（a）传统的 Internet 流量模型　　（b）P2P 流量模型

图 11.3　传统的 Internet 流量模型和 P2P 流量模型的区别

11.4.2 P2P技术

1．关键技术

P2P 是一种基于互联网环境的新的应用型技术，主要为软件技术。

（1）对于互联网上众多计算机，P2P 应用比其他应用要更多考虑那些低端 PC 的互连，它

们不具备服务器那样强的连网能力，同时对于以往的 P2P 应用技术，现在的硬件环境已经更为复杂，这样在通信基础方面，P2P 必须提供在现有硬件逻辑和底层通信协议上的端到端定位（寻址）和握手技术，建立稳定的连接。涉及的技术有 IP 地址解析、NAT 路由及防火墙。

（2）在应用层面上，如果两个 Peer 分别代表两家不同的公司，而且它们已经通过互联网建立连接，那么一方的信息就必须为另一方所识别，所以当前互联网上关于数据描述和交换的协议（如 XML、SOAP、UDDI 等）都是一个完善的 P2P 软件所要考虑的。

（3）有通信就要有安全保障，加密技术是必须要考虑的。

（4）其他需考虑的有如何设置中心服务器、如何控制网络规模等。

2．P2P技术与现有互联网技术比较

目前，互联网的主要技术模式是 S/C 方式，此方式要在互联网上设置拥有强大处理能力和大带宽的高性能计算机，配合高档的服务器软件，再将大量的数据集中存放在上面，并且要安装多样化的服务软件，在集中处理数据的同时可以为互联网上的其他 PC 服务，提供或接收数据，提供处理能力及其他应用。对于一台与服务器联机并接受服务的 PC 来说，这台 PC 就是客户机，其性能可以相对弱小。而 P2P 技术的特征之一就是弱化了服务器的作用，甚至取消服务器，任意两台 PC 互为服务器，同时又是客户机，即对等。

3．P2P技术严格地说是一种网格

网格的定义：网格是在网络上运行的软件基础设施，是连接集成不同硬件系统、软件系统、应用系统的纽带和黏合剂。

4．P2P技术特性

（1）既是服务器又是客户机，如何表现取决于用户的要求，网络应用由使用者自由驱动。

（2）信息在网络设备间直接流动，高速及时，降低中转服务成本。

（3）构成网络设备互动的基础和应用。

（4）在使网络信息分散化的同时，相同特性的 P2P 设备可以构成存在于互联网这张大网中的子网，使信息按新方式又一次集中。

11.4.3 P2P应用

1．P2P内容共享

P2P 内容共享即基于 P2P 协议的文件共享。典型的应用软件有 BT、eDonkey、PP 点点通、Gnutella、FastTrack、酷狗（Kugoo）、迅雷、DirectConnect、AppleJuice、百宝、百度下吧、百兆等。

这是目前被广泛使用、同时也是头号带宽杀手的应用协议。

2．P2P通信协作

P2P 通信协作包括协同工作、互联网电话、即时通信 S 和移动通信。P2P 即时通信系统采用对等连接模式 P2P，可以提供异步、并行、可靠和近似实时通信。

即时信息类，如腾讯 QQ、微软 MSN、YahooMessger 等。

网络电话类，如 Skype 等。

3．P2P协同计算

P2P 协同计算包括协作计算、网格和数据内容网格。采用 P2P 和 Grid 融合产生数据内容网格，用 P2P 技术建立数据网格是最有吸引力和实际的方法。综合 P2P 技术建立内容网格，在网格中数据、内容是自动分布的，用户可以接入最近的数据。视频内容网格，以分布式存

储提供视频点播业务。

4．P2P网络媒体

电视视频节目除现场直播以外，都是事先录制好存储在服务器中的。点播是一种工作模式，但是它占用网络资源太多。P2P 为网络电视媒体提供了一个新的工作模式，用户可以先用 P2P 方式下载内容并存储在自己的计算机中，再回放观看。

网络电视类应用，如 PPStream、PPLive、沸点、Recool、QQLive 等。

11.4.4 P2P前景展望

从 P2P 技术的发展轨迹来看，它与互联网技术的发展是一致的，即从技术导向逐渐转向市场导向，从专属用户逐渐转向普通用户。这也意味着，这些技术的影响力将从纯技术层面转向经济、文化与社会层面。

P2P 技术既然可以为个人对个人的信息交流与共享提供方便，自然也能为媒体对媒体的信息交流与合作提供可能。P2P 技术也可能成为媒体间的交流与合作的新平台，也可能加速媒体形态的演化。对于媒体机构来说，现在能感觉的似乎更多的是潜在的威胁，因为它们在传统媒体以及网络媒体中的中心特权地位会受到挑战，但是，从另一个角度来看，如果媒体机构把自己视为一个普通的信息产品的生产者，也许就能从 P2P 技术中找到新的希望。

本 章 小 结

本章主要讲述了以下内容。

（1）多层交换技术是在网络模型中的第三层以上实现了数据包的高速转发。

（2）三层交换技术也称为 IP 交换技术、高速路由技术等。这是一种利用第三层协议中的信息来加强第二层交换功能的机制。第三层交换的目标是，只要在源地址和目的地址之间有一条更为直接的第二层通路，就没有必要经过路由器转发数据包。

（3）第四层交换技术利用第三层和第四层包头中的信息来识别应用数据流会话，第四层交换机可以做出向何处转发会话传输流的智能决定。

（4）第七层的智能性能够对所有传输流和内容进行控制。由于可以自由地完全打开传输流的应用/表示层，仔细分析其中的内容，因此可以根据应用的类型而非仅根据 IP 和端口号做出更智能的负载均衡决定。

（5）IPv6 是“互联网协议第 6 版”的缩写。IPv6 是由 IETF 设计的下一代互联网协议，目的是取代现有的互联网协议第 4 版（IPv4）。IPv6 能够解决 IPv4 的许多问题，如地址短缺、服务质量保证等。

（6）IPv6 报头的结构比 IPv4 简单得多。IPv6 的 128 位地址是以 16 位为一分组，每个 16 位分组写成 4 个十六进制数，中间用冒号分隔，称为冒号分十六进制格式。

（7）IPv4 到 IPv6 的过渡采用的技术有：隧道技术、网络地址转换/协议转换技术、IPv6/IPv4 双协议栈技术、应用服务系统（DNS）过渡技术等。

（8）IPv6 的应用包括从语音、数据到视频以及无线通信等。

（9）网格（Grid）是把整个 Internet 整合成一台巨大的超级计算机，实现计算资源、存储资源、数据资源、信息资源、知识资源、专家资源的全面共享。

（10）在科学研究、企业信息处理、电子政务以及个人娱乐等社会生活的各个领域都活跃

着网格技术的身影。

（11）P2P 是“Peer-to-Peer”的缩写，称为对等网。P2P 是一种分布式网络，其中的参与者共享他们所拥有的一部分硬件资源，这些共享资源需要由网络提供服务和内容，能被其他 Peer 直接访问而无需经过中间实体。

（12）P2P 的应用包括内容共享、通信协作、协同计算和网络媒体等多个领域。

思 考 题

1．什么是三层交换？常用的三层交换技术有哪些？

2．为什么要采用 IPv6？IPv6 的地址如何表示？

3．IPv4 到 IPv6 的过渡如何实现？

4．简述网格技术。

5．什么是 P2P 网络？其应用和发展前景如何？

参 考 文 献

[1] 徐其兴．计算机网络技术及应用（第 3 版）．北京：高等教育出版社，2008.

[2] Andrew S.Tanenbaum．计算机网络（第四版）．北京：清华大学出版社，2004.

[3] 雷震甲．网络工程师教程（第 2 版）．北京：清华大学出版社，2007.

[4] 吴功宜，吴英．计算机网络技术及应用（第 3 版）．北京：电子工业出版社，2004.

[5] 谢希仁．计算机网络（第四版）．北京：电子工业出版社，2004.

[6] 石炎生．计算机网络工程实用教程．北京：电子工业出版社，2007.

[7] 睢丹．网络设备基础教程与实验指导．北京：清华大学出版社，2007.

[8] 戴有炜．Windows Server 2003 Active Directory 配置指南．北京：清华大学出版社，2004.

[9] 戴有炜．Windows Server 2003 用户管理指南．北京：清华大学出版社，2004.

反侵权盗版声明